(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 907 120 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
07.04.1999 Bulletin 1999/14

(51) Int. Cl.[6]: **G06F 1/00**, H04L 9/32

(21) Application number: **98118486.4**

(22) Date of filing: **30.09.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **02.10.1997 US 957986**
09.04.1998 US 57966

(71) Applicant:
Tumbleweed Software Corporation
Redwood City, California 94063 (US)

(72) Inventors:
- **Smith, Jeffrey C.**
  Menlo Park, CA 94025 (US)
- **Bandini, Jean-Christophe**
  Cupertino, CA 95014 (US)
- **Shoup, Randy**
  San Francisco, CA (US)

(74) Representative:
Diehl, Hermann, Dr. Dipl.-Phys. et al
DIEHL, GLÄSER, HILTL & PARTNER
Patentanwälte
Augustenstrasse 46
80333 München (DE)

(54) Method amd apparatus for delivering documents over an electronic network

(57) A method and apparatus are provided for securely delivering documents over an electronic network (18) while preserving document formatting. The invention also provides security that restricts access to the system to an authorized user. A document is sent from a sending computer (14) to a dedicated server (22), using a send client application (20). A dedicated server (22) stores the document (16) and forwards an electronic notification to a receiving device (24,26,28). The stored document is downloaded from the dedicated server (22), using a receive client application (30), in response to the notification. The receive client application (30) permits the recipient to receive, view, print, and/or manipulate the document. A sender driven certificate enrollment system (1342) and methods of its use are also provided, in which a sender (1352) controls the generation of a digital certificate (1345) that is used to encrypt and send a document to a recipient (1370) in a secure manner.

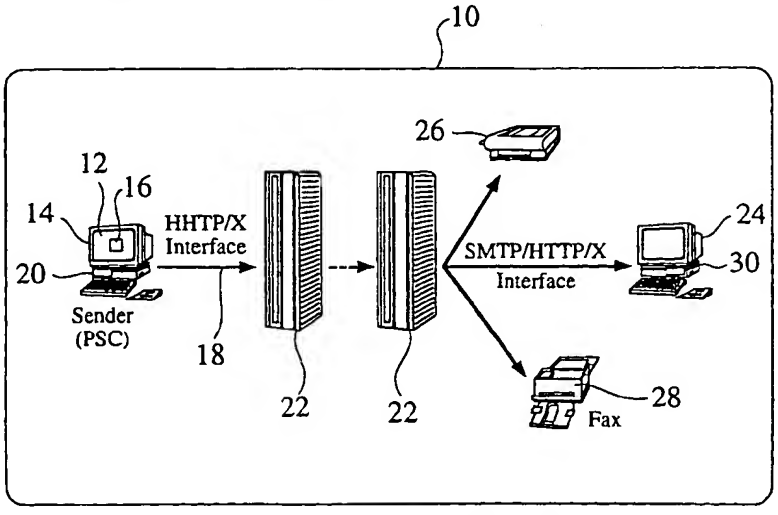


Fig. 5

EP 0 907 120 A2

Secret key encryption, sometimes referred to as symmetric key cryptography, employs a technique of scrambling information to prevent unsolicited access, using a unique, secret key 1214.

[0016] Figure 2 is a block diagram of secret key decryption 1210b, wherein the same, unique secret key 1214 is required to unscramble 1222 the encrypted document 1220, to reproduce a copy of the original document 1212. Without access to the secret key 1214, an encrypted document 1220 remains secure from tampering.

[0017] One potential issue with secret key encryption 1210a and 1210b is the challenge of distributing the secret key 1214 securely. For example, suppose a sender uses secret key encryption to encrypt a document 1212, and then sends a recipient the encrypted document 1220. The recipient needs the secret key 1214 to decrypt 1222 the encrypted document 1220. If the secret key 1222 is sent over a non-secure channel, then the integrity of the security is compromised. For most applications, telephone or fax provides a secure enough means of delivering secret keys 1214, while the encrypted document 1220 can be delivered over the internet using the Posta™ document delivery system. In some instances, however, senders and recipients require a more robust or convenient means of distributing a secret key 1214.

[0018] Public key encryption facilitates a more robust, and typically a more convenient means, of delivering information securely. With public key encryption, each recipient owns a pair of keys, called a public key and a private key. The key pair's owner (the recipient) publishes the public key, and keeps the private key a secret.

[0019] Fig. 3 is a block diagram of public key encryption 1230a, wherein a document 1312 is encrypted, or scrambled 1234, with a public key 1332, producing an encrypted document 1336. To send information to a recipient, a sender uses the published public key 1332 of the intended recipient to encrypt 1234 the information, and then the recipient uses their own private key 1334 (Fig. 4) to decrypt the information. Hence, the private key 1334 (which is necessary to decrypt the information) is not distributed. Fig. 4 is a block diagram of private key decryption 1230b, wherein the private key 1334 is required to unscramble 1238 the encrypted document 1336, to reproduce a copy of the original document 1312. Without access to the private key 1334, an encrypted document 1336 remains secure from tampering.

[0020] Public key encryption 1230a and 1230b typically exploits a mathematical relationship between the public and private keys 1332, 1334, which allows a public key 1332 to be published, without risking the derivation of the private key 1334 from the published public key 1332.

[0021] Public key encryption algorithms are typically complex, and hence may be too time consuming to be of practical use for many users. Secret key encryption 1210a, 1210b is typically much faster than public key encryption 1230a, 1230b, but requires the transmission the secret key 1214 from the sender to the recipient.

[0022] In a digital envelope system, a user encrypts a document 1212 with a secret key 1214, and then encrypts the secret key 1214 with the public key 1332 of the intended recipient. The recipient of the encrypted document 1220 then uses their private key 1240 to decrypt the secret key 1214, and then uses the secret key 1214 to decrypt the document.

[0023] It is often useful to verify if a document has not been altered during transmission, or to verify who sent or received a given document. Hashing algorithms (or message digests) and public key technologies facilitate solutions to document integrity and transport verification.

[0024] Digital certificates can also be used to provide enhanced security for encrypted information. Suppose a recipient owns a public/private key pair and wishes to publish the public key 1332 so others can use the public key 1332, either to encrypt information to be sent to the recipient, or to verify the digital signature of the recipient. A secure technique for the recipient to publish the public key 1332 is to register the public key 1332 with a trusted authority. The trusted authority can then certify that a particular public key 1332 belongs to the recipient. A digital certificate connects a recipient, or other entity, with a particular public key 1332.

[0025] A digital certificate, as disclosed later, is a record of a public key and an identity, and the association of the two as attested to by a third party by means of a digital signature. The private key is not in the certificate, but only one private key can match a given public key. A public/private key pair is actually a pair of numbers with the following properties.

- The private key cannot be derived easily from the public key; and
- The public key can be used to cipher data which can only be deciphered by knowing the private key (some public keys algorithms, such as RSA, also have the inverse property, which makes them suitable for use a digital signatures).

[0026] A trusted or certificate authority issues and maintains digital certificates.

[0027] The disclosed prior art systems and methodologies thus provide some methods for the encryption and secure delivery of documents, but fail to provide a simple digital certificate generation and enrollment system that is implemented and controlled by a sender. The development of such a digital certificate system would constitute a major technological advance.

[0028] It is therefore the object of the present invention to provide an apparatus for managing and delivering documents, which overcomes the drawbacks of the prior art. This object is solved by the apparatus for man-

tional commands.

[0040] The invention also provides a security framework that restricts system access to an authorized user. The types of security supported include authentication layers, secure socket layers, password protection, private key encryption, public key encryption, and certificate authentication. The security framework can be implemented as one or more modules, and can be incorporated into at least one of the send client application, the receive client application , and the CUI.

[0041] A sender driven certificate enrollment system and methods of its use are provided, in which a sender controls the generation of a digital certificate, which can be used to encrypt and send a document to a recipient in a secure manner. The sender compares previously stored recipient information to gathered information from the recipient. If the information matches, the sender transfers key generation software to the recipient, which produces the digital certificate, comprising a public and private key pair. The sender can then use the public key to encrypt and send the document to the recipient, wherein the recipient can use the matching private key to decrypt the document. In a preferred embodiment, a server is interposed between the sender and the recipient, to provide increased levels of system security, automation, and integrity.

[0042] The above mentioned and other features of the present invention and the invention itself will be understood by the reference to the following detailed description of the preferred embodiments of the invention, when considered in conjunction with the accompanying drawings, in which:

Fig. 1 is a block diagram of secret key encryption of a document;

Fig. 2 is a block diagram of secret key decryption of a document;

Fig. 3 is a block diagram of public key encryption of a document;

Fig. 4 is a block diagram of private key decryption of a document;

Fig. 5 is a diagram of a document delivery system according to the invention;

Fig. 6 is a view of an application window according to the invention;

Fig. 7 is a view of an application window showing document activities according to the invention;

Fig. 8 is a view of a package window, according to the preferred embodiment of the invention;

Fig. 9 is a view of a recipient's window according to the invention;

Fig. 10 is a view of a CUI application window according to the invention;

Fig. 11 is a view of a CUI package window according to the invention;

Fig. 12 is a view of a CUI options page according to the invention;

Fig. 13 is a view of a CUI tracking search page according to the invention;

Fig. 14 is a view of a CUI tracking report preferences dialog according to the invention;

Fig. 15 is a view of a recipient summary tracking report in basic format according to the invention;

Fig. 16 is a view of a recipient detail tracking report in Basic Format according to the invention;

Fig. 17 is a view of a recipient detail tracking report in billing code format according to the invention;

Fig. 18 is a view of a group account manager account - view members window according to the invention;

Fig. 19 is a view of a billing codes window according to the invention;

Fig. 20 is a view of an edit billing codes dialog according to the invention;

Fig. 21 is a view of an add billing codes dialog according to the invention;

Fig. 22 is a view of a create invoice page, according to the invention;

Fig. 23 is a view of a basic invoice report window according to the invention;

Fig. 24 is a view of a billing preferences dialog according to the invention;

Fig. 25 is a view of an invoice report in spec invoice format according to the invention;

Fig. 26 is a view of an invoice report in billing code invoice format according to the invention;

Fig. 27 is a view of a mail list page according to the invention;

Fig. 28 is a view of a mail list detail page according

the intended recipient can copy the URL directly from the notification message, and paste it into a Web browser on the receiving computer. The Web browser then retrieves the document from the dedicated server. In alternative embodiments of the invention, the receive client application is any other software application capable of retrieving the stored document from the dedicated server while maintaining document formatting.

[0051] The send client application is readily installed on a computer from a CD-ROM, or by downloading from the Web. For example, a user who already has an account with a dedicated server provider can configure the send client application with the appropriate account information. A user who does not have such an account is directed to a URL that has the information for setting up an account.

[0052] The send client application is accessed via an application window displayed on the sending computer's desktop. The application window is displayed once the account information is properly configured. Fig. 6 is a view of an application window 32 according to the preferred embodiment of the invention.

[0053] The main function of the application window is to view the status of, and to manage send client application activity. The application window also serves as a launching pad to reach the various functions of the send client application and the configuration user interface CUI (discussed below).

[0054] In the preferred embodiment of the invention, the application window displays a main tool bar 34 for accessing main functions of the send client application. One such function is the selectable button for new package 36. Clicking on new package opens a new package window (discussed below), which allows a user to initiate a delivery of a document. Clicking on the open button 38 opens either a saved delivery parameter or a saved package window (discussed below).

[0055] In the preferred embodiment, the main tool bar 34 includes buttons that are Internet shortcuts to CUI functions. Clicking on such button launches the user's Web browser and displays the appropriate page in the CUI. In the preferred embodiment of the invention, no additional login is required in this process. Examples of such buttons include tracking 40, account 42, billing 44, and mail lists 46 buttons.

[0056] Buttons may also be provided for send client application settings. For example, a preferences dialog accessed via a setup button 48 permits the user to specify dedicated server and proxy server account information. The user can also specify whether or not to use a low-level secure communications protocol, such as Secure Socket Layer (SSL) to secure the connection between the desktop and the dedicated server for all transmissions.

[0057] The send client application can access the local address books of supported applications. In the preferred embodiment of the invention, the user selects the setup button 48 and is presented with a pull-down menu which lists the address books supported by the invention. The user then selects the desired address book file.

[0058] A stop button 50 is used to stop transmission of all information to the dedicated server. In the preferred embodiment of the invention, once clicked, the stop button remains depressed. To resume transmission, the user clicks on the button again, and it returns to a raised position.

[0059] The menu 52 lists operational commands for the send client application. In the preferred embodiment of the invention, the file menu 54 contains commands that have the same functionalities as buttons on the main tool bar 34. Other commands provide information regarding the send client application, or are Internet shortcuts to functions of the CUI. In Fig. 6, the menu includes listings for edit 56, package 58, CUI 60, and help 62.

[0060] The application window also displays a package manager 64 that lists all document activities initiated during an application session. The package manager is an area, or set of fields in the body of the application window which lists all document activities that have been initiated during a send client application session. When the send client application is first launched, the package manager field is empty. However, as documents are sent, they are listed in the package manager.

[0061] Fig. 7 is a view of an application window 32 showing document activities 72 according to the preferred embodiment of the invention. The package manager may display the recipient(s) 66, the subject 68, and the status 70 of the delivery. The status of an active delivery may be represented as a dynamic percentage of upload completed. Other possible status labels include "completed," "error," "pending," and "on hold."

[0062] Documents may be listed, for example, in processing, or reverse processing orders. In the preferred embodiment of the invention, the document currently being processed 74 is presented in bold characters. In alternate embodiments, the current document is indicated by other means, including highlighting, flashing, or color, or is unmarked.

[0063] Clicking on a listed document 76 highlights that listing and selects the document. Multiple documents may be selected at one time. Once a document is selected, the user can use the menu 52, for example, to hold, edit, or delete the document.

[0064] A hold prevents a pending document from being processed. The document is held in a queue until it is deleted or the hold is removed. In the preferred embodiment of the invention, any or all documents in the list can be deleted. A current send is completely aborted, and an already-processed document is deleted from the window.

[0065] Editing opens a document within a new package window (discussed below). The user can then edit the document and resubmit it for sending. If a document

saved package window may then be re-opened for future use.

[0082] Saved delivery parameters can be used on a recurring basis across sessions. From a package window, a user can save delivery parameters including specified send options, an address list, and/or a fixed subject or message. To save delivery parameters, a user clicks on the save parameters button 96. A dialog box prompts the user to specify a name and location for the delivery parameters to be saved.

[0083] If the saved delivery parameters contain an address list, the user can initiate a delivery by clicking and dragging a document icon onto the saved delivery parameter icon. The document provides the remaining information required for a delivery, and the send is initiated automatically. The saved delivery parameter thus serves as a dedicated mail chute to a specific set of recipients.

[0084] The existing send options may be modified or confirmed before launching the delivery. A window displaying all send parameters is opened, and the user can modify parameters or append a message before sending the document. In the preferred embodiment of the invention, the user is prompted to save any modifications to send options or existing address lists upon closing the package window.

[0085] If the saved delivery parameters do not include an address, clicking and dragging a document onto the saved delivery icon opens a package window. The saved send options and name of the document are specified in the package window. The user must specify a recipient before the document can be sent.

[0086] Saved delivery parameters are opened by clicking on the associated icon, or by selecting the appropriate main tool bar 34 or menu items. The settings are displayed in a package window and are completed or modified for a delivery. If the send client application is not open, opening the saved delivery parameters opens the application window as well as a package window. Modifications to the saved delivery parameters are preserved by replacing the existing saved parameters, or by creating a new saved delivery parameters file under a different name.

[0087] If unsaved changes have been made to the saved delivery parameters, the user is prompted to save the changes upon closing the package window. A sender can add an address list to an existing saved delivery parameter that did not previously contain an address list. The settings of the package window are saved using the "save settings as default" button 116.

[0088] Fig. 9 is a view of a recipients window according to the preferred embodiment of the invention. The recipients window 118 is used to select the recipient's name from an address book or pre-defined mail list.

[0089] In the preferred embodiment of the invention, a pull-down menu 120 allows the user to access addresses in a local address book or a mail list. For example, selecting mail list in the pull-down menu and clicking on the refresh button 122 populates the list box 124 with the names of the mail lists stored on the dedicated server for the account for which the send client application is configured. Selecting local address book and clicking on the refresh button populates the list box with addresses from the address book specified in the preferences dialog.

[0090] Each time the recipients window is opened, the send client application displays a previously cached list of addresses. Clicking on refresh forces a refresh of the list from the appropriate source. The send client application presents the last selected source for the next send, both within and across sessions. The cancel button 135 cancels the recipients window display.

[0091] A user can select items from the list box 124 and click the "To" arrow button 126 to specify the selections as recipients. In the preferred embodiment of the invention, control-click allows selection of multiple items and shift-click selects a range of items. Recipients are presented in the recipients box 128. Recipients listed in the recipients box list are selected and removed by clicking the delete button 130 or by hitting keyboard backspace or delete keys.

[0092] When the user clicks on the "OK" button 132, items in the recipients box list are displayed in the "To:" field 110 of the package window 78 (see Fig. 8). In the preferred embodiment of the invention, mail lists have the prefix "list:" prepended to them. A user can also delete or modify recipient addresses from the "To:" field of the package window.

[0093] The specified document delivery parameters may be stored in a storage module for later modification and/or use. In the preferred embodiment of the invention, the send client application and the package window are accessed by selecting their representative icons (not shown) from the sending computer's desktop.

[0094] A configuration user interface is provided for directly invoking and customizing the dedicated server. The CUI is accessed via a CUI application window displayed on a managing computer desktop. Alternatively, the CUI is accessed through any Web browser application that supports tables, or accessed through the send client application. Fig. 10 is a view of a CUI application window 140 according to the preferred embodiment of the invention.

[0095] In the preferred embodiment of the invention, the CUI is an HTML interface for invoking and customizing the dedicated server via a Web browser. This HTML interface includes modules for sending the document, tracking the document, accessing information associated with the document delivery account, managing billings for the document delivery, and managing mail distribution lists.

[0096] The CUI offers different sets of functions, depending on the user and type of account used. Individual account holders, group account managers, and group members see slightly different interfaces and are able to access and manipulate varying sets of data.

preferred embodiment of the invention. The preferred embodiment of the invention supports security and encryption features permitted under current law for use in the United States. Alternative embodiments of the invention comply with any security and encryption requirements for software applications intended for export from the United States.

[0113] The CUI user may specify a password 206 that a recipient must provide to access a document. The user may also specify confirm password 208, encrypt document 210 and require SSL to receive 212. The password may be used as a secret key to encrypt the document on the server. This provides a higher level of security while the document is stored on the server. If the encrypt document function 210 is selected but the user has not specified a password, the CUI transmits an error message when the user attempts to apply the settings.

[0114] The billing code option 214 allows users to select a billing code, including "None" from a pull-down menu. The list is defined and maintained in the billing module of the CUI (see Fig. 19). The "Billing Code" text link brings users to the billing section of the CUI. Users may thereby view and manipulate billing codes.

[0115] Clicking on the reset button 216 restores the default settings. Alternatively, the current settings may be saved 218 as the default. Once the options are set, the user uses the Update button 220 to return to the package window 170. A delivery is then initiated by clicking on the send button 188.

[0116] Tracking is accessible from the tracking button 144 on the persistent main tool bar 154. The tracking search function is used to query the CUI database for information about deliveries sent from an account. A sender can therefore find out whether a recipient has received a particular document. The database archive can also be searched for records of past transactions.

[0117] Fig. 13 is a view of a CUI tracking search page 222 according to the preferred embodiment of the invention. The secondary navigation from the secondary tool bar 156 includes log 224, search 225, report 226, preferences 228, and help 158. The current function 192, search 225, is identified. The tracking button on the main tool bar displays a record of all deliveries sent from the account as a delivery log (not shown).

[0118] Account managers are permitted to track all deliveries initiated from a group account. Group members are permitted to track only those deliveries initiated personally by the member.

[0119] The format of the delivery log is specified in tracking preferences (see Fig. 14). The format chosen applies to both the delivery log and the tracking report (see Figs. 15-17). The preferred embodiment of the invention includes navigation buttons to permit the user to access previous, or subsequent log pages. Information regarding an individual delivery may be displayed on the delivery log, along with an indication of the total number of deliveries logged.

[0120] The subject of each listing in the log links to a package detail report (not shown) about the specific delivery. A detail report contains send parameters of each delivery, including a link to the document if not expired, the mimetype, and the message. The detail report also contains the status of the delivery to each recipient, and the charges applied to the transaction. Users can click on log 224 on the secondary tool bar 156 to return to the top level log.

[0121] The search function allows users to pinpoint information about, and the status of, a specific delivery or set of deliveries. The user specifies any combination of search criteria to identify the deliveries of interest. If multiple criteria are specified, the search engine performs a logical "AND" search among all the criteria.

[0122] In the preferred embodiment of the invention, the search page graphical user interface (GUI) is simplified. A short list 230 of common searchable fields is presented on the Search page. The short list contains five search criteria:

[0123] The "To:" field 232 allows a user to search by the intended recipient's full or partial E-mail address of the recipient. Partial e-mail addresses allow the user to search by domain name.

[0124] The "From:" field 234 allows an account manager to search according to the originator of the delivery. The account manager selects a member's e-mail address from a pull down menu. For group members and individual account holders, this given user's e-mail is provided and cannot be changed.

[0125] The "Subject:" field 236 allows a user to enter keywords which may be found in the subject field of a document.

[0126] The "Document:" field 238 allows a user to perform a text search on the name of the document. A user can type in the name of the document, or browse through the list of documents to select a document.

[0127] The "Send date:" field 240 allows a user to search for deliveries sent on, before, or after a specific date.

[0128] Clicking on the search button 242 initiates the query and returns a report with all deliveries matching the query. Clicking on the reset button 246 clears the form to its default setting.

[0129] Clicking on a "More Options..." button 248 at the bottom of the short form brings the user to a page having a second, expanded list (not shown) of searchable fields, including all fields from the short list. In the preferred embodiment, the additional fields in the expanded list include:

[0130] The billing code: field allows a user to select from a pre-defined list in a pull down menu.

[0131] The "Delivery status:" field allows a user to select from a menu of delivery statuses. Delivery status options include: any, received, not received (includes both failed notification and not picked up), confirmed, not confirmed, pending notification and failed notification. The user may also search document expiration,

existing password and the desired new password, and must confirm the new password. The manager submits the new password by clicking on Update.

[0150] In the preferred embodiment, the information page also includes a field which informs the manager when the password was last changed. If the password has never been changed, this field presents the creation date of the account. A link may also be provided to a server manager who is authorized to make changes to accounts.

[0151] Managers can view a list of members by clicking on the members text link on the Information page, or by selecting the view members function of the secondary tool bar 156. Fig. 18 is a view of a group account manager account - view members window 288, according to the preferred embodiment of the invention. In one embodiment, managers use a link (not shown) to Preferences (not shown) where the managers can specify the format, the number of rows per page, and the sorting order of the View Members table.

[0152] The view members page displays the name 290 of the group account, and the number 292 of the members displayed out of the total number. The list of members includes the account manager, and is presented in a table which lists the member account names 294, the member names 296, the date created 298, and the date last accessed 300. Clicking on a member's name brings up a "Mailto:" box (not shown), preaddressed to the member.

[0153] Clicking on the account name allows managers to view and edit individual member account information. This information is displayed on a member account information page (not shown) which is similar in format to the group account information page. Basic member account information includes the following (editable information is noted):

- group account
- member account (editable)
- date created
- date last accessed

Member information

[0154]

- member name (editable)
- e-mail address (editable)

[0155] Managers cannot view the member's password, but can change the password on the member account information page by specifying a new password and confirming it. The date of the last password change (not shown) by either manager or member is also displayed. Any changes made to the information on this page can be submitted by clicking on update (not shown). Reset (not shown) restores the previously stored information.

[0156] Member accounts can be completely deleted by clicking on a delete button on the member account information page. Prior to deleting the account, the dedicated server posts a confirmation page notifying the manager of the impending action and requesting confirmation before proceeding. When the member account is updated or deleted, an updated view members window is displayed.

[0157] Managers can add members by clicking on the add member link in the secondary tool bar 156. A form (not shown) is displayed prompting the account manager for the information required to create a member account. The form indicates the group account to which the member is added, and the number of the member out of the maximum total members allowed. The information required includes:

- member account name (created by the manger)
- member's name
- member's e-mail address
- password (and confirm password)

[0158] Clicking on add (not shown) creates a new account and returns the manager to an updated view members window. Clicking on reset (not shown) clears the form.

[0159] Because individual accounts have no group members aside from the account holder, such individual account holders do not have member information or functions. The secondary tool bar 156 includes only Information (not shown) and help (not shown.) The information displayed from the account information page is the same as that available from the group account information page, except for the number of current members.

[0160] Member account holders also do not have member management functions, and the secondary tool bar includes only information (not shown) and help (not shown). Member account information contains the same basic information as that viewed by managers. However, members are only able to edit e-mail address information.

[0161] In the preferred embodiment, members can change their own passwords on the member account information page. They must enter the current password, the new password, and then must confirm the new password. However, in alternative embodiments, members may only be able to change their passwords via the account manager.

[0162] The billing button 148 on the main tool bar 154 gives access to billing code mode management and invoice functions. Clicking on the billing button displays a table 320 of defined billing codes. Fig. 19 is a view of a billing codes window 308, according to the preferred embodiment of the invention.

[0163] Secondary navigation for billing on the secondary tool bar 156 includes billing codes 310, add codes 312, create invoice 314, view Invoice 316, preferences

first column is description and the list is sorted by description. The user specifies the number of rows displayed 402 per page.

[0184] The user also specifies the rate 404 to charge clients. This rate can be a flat charge 408, or may include a percentage mark-up 406 on top of the costs charged by the user's Internet services provider. The information displayed in the billing preferences dialog can be updated 405 or refreshed 407.

[0185] For the invoice report, the user may select a predefined format 410, or define 412 a new format. In the preferred embodiment, the user selects from three predefined formats the basic invoice, spec invoice, and billing code invoice formats. The basic invoice format has previously been shown in Fig. 23.

[0186] Fig. 25 is a view of an Invoice report in spec invoice format according to the preferred embodiment of the invention. The spec invoice 414 displays the total number 416 of recipients for each delivery as well as the size 418 of the document. This information is sorted chronologically.

[0187] Fig. 26 is a view of an invoice report in billing code invoice format according to the preferred embodiment of the invention. The billing code invoice format 420 is sorted by billing code 422, as well as by date.

[0188] The CUI allows publishers and other users to create and manage distribution lists. Fig. 27 is a view of a mail list page 424 according to the preferred embodiment of the invention. Mail list functions are accessible from the main tool bar 154. Secondary navigation includes mail list 426, create list 428, preferences 530 and help 158.

[0189] There are two levels of mail lists for group accounts, i.e. group and personal. Group lists are managed by the account manager and are accessible to all group members. A group member can define a personal list accessible only by that group member. Each member can specify which set of lists to use in their mail list preferences.

[0190] Clicking on the mail list button 150 on the main tool bar 154 displays a table 432 listing existing mail lists 434. The table also presents the total number 436 of recipients on each mail list and the date 438 the mail list was most recently modified. The preferences settings 440 are also displayed.

[0191] In mail list preferences (not shown), the user specifies whether to sort the items by the name of the mail list or by date. Current preferences are displayed in the mail lists dialog. Next and previous buttons (not shown) may be provided to navigate between pages of mail lists.

[0192] Clicking on the hot-linked name 442 of a mail list brings up a mail list detail for the selected mail list. Fig. 28 is a view of a mail list detail window 444, according to the preferred embodiment of the invention.

[0193] The mail list detail page displays general information about an existing mail list and allows the user to view and manage mail list addresses. Group members cannot manipulate group mail lists. Therefore, the mail list detail of group lists does not display fields for editing. Group members can, however, edit personal mail lists.

[0194] Account Managers can manipulate group mail lists. The detail 444 presented to account managers displays the name 446 of the mail list in an editable form. To rename the list, the user changes the name in the form and clicks on the update button 448. Users may also delete 450 the entire mail list or add addresses 452 by clicking on the appropriate button. The total recipients 454 and date last modified 456 are also displayed.

[0195] The detail also displays the mail list addresses 458. In the preferred embodiment of the invention, the first page of the complete address list is displayed in accordance with the number of rows per page specified in the mail list preferences. The detail indicates which addresses out of the total are displayed. Next and previous links (not shown) may be provided to navigate between multiple pages of addresses.

[0196] The user can also view a select set of addresses by specifying a query in the field 460 provided. For example, an e-mail address or a portion of an address such as a domain name can be specified. Clicking on the view button 462 then displays a table 464 of matching addresses 458. The table indicates which addresses 466 out of the total matching set of addresses are displayed.

[0197] The user edits or deletes individual addresses in the table by clicking on the appropriate address. An edit page (not shown) with update and delete buttons is then displayed. When the address is updated or deleted, users are returned to an updated mail list detail page.

[0198] From the detail page, users can also delete multiple addresses at a time. Clicking on the "delete items on page" button 468 deletes all the addresses in the table. Clicking on "delete all matching items" 470 deletes all items which matched the query, whether or not the addresses are visible on the current page. A warning message asking the user to confirm the action is displayed before the dedicated server actually deletes the addresses. Once the addresses are deleted, the detail page is immediately updated and presented to the user.

[0199] Clicking on the add addresses button 452 in the mail list detail 444 displays the add addresses page. Fig. 29 is a view of an Add Addresses window 472 according to the preferred embodiment of the invention. The name of the current mail list 474 is displayed at the top. The name is also linked to the mail list detail page.

[0200] The user can add additional addresses by manual entry 476, by uploading them from a file. The user can enter a file name 478, or use the browse button 480 to search all files. Names may also be obtained from an existing mail list 482 and merged with the current mail list. The additional addresses are added 484 to the current address list or replace 486 the current list. After the names are submitted, the users are returned

secure document delivery stems from the challenge of encrypting a document 1312 with the public key 1332 of the intended recipient 1370. In particular, the intended recipient 1370 of a document may not have a digital certificate 1345. In the absence of a digital certificate 1345 of the recipient 1370 which is accessible by the sender 1352, the sender 1352 of a document 1312 cannot encrypt the document 1312 with the recipient's public key 1332, and hence cannot be assured that the document 1312 can be protected from unsolicited access. The sender driven certificate enrollment system 1342 allows the sender 1352 of a document 1312 to initiate the process of dynamically generating a digital certificate 1345 for the intended recipient 1370, thereby imposing minimum requirements for the intended recipient 1370.

[0215] The sender driven certificate enrollment system 1342 transfers the burden of certificate generation from the recipient 1370 of a given document 1312 to the sender 1352. The sender driven certificate enrollment system 1342 exploits the fact that, in the context of document delivery, often the sender 1352 of a document 1312 has unique and specific information regarding the intended recipient 1370. Suppose, for example, an attorney sends a document to a client 1370. The attorney 1352 likely has a record associated with the client 1370 which contains specific information, such as the client's e-mail address, physical address, telephone number. The client record may also contain confidential information, such as the client's social security number, drivers license number, or even credit information.

[0216] Typically, it is this type of confidential information which is utilized to authenticate a given individual or entity 1370, and hence generate a digital certificate 1345. Highly confidential and specific information yields a high level of authentication, and hence a secure digital certificate.

[0217] Therefore, the sender driven enrollment system 1342 exploits the fact that the sender 1352 often knows significant and confidential information regarding an intended recipient 1370 of a document 1312. The use of this confidential information by the sender 1352 to generate a digital certificate 1345 minimizes the burden imposed on the recipient 1370 to confirm their identity. The digital certificate 1345 is then utilized by the sender 1352 to securely send the document 1312 to the intended recipient 1370.

[0218] System Implementation. In the example above, a sender attorney 1352 wishes to send a confidential document to an intended recipient client 1370. For a client 1370 that does not currently have a digital certificate 1345 accessible to the attorney 1352, the attorney 1352 can invoke the sender driven enrollment system 1342 to generate a digital certificate 1345 for the client 1370.

[0219] First, the sender driven enrollment system 1342 checks or queries a database 1346 to determine if a digital certificate 1345 exists for the recipient client 1370. If not, the sender driven enrollment system 1342 conducts a database query to pull up a record for the client 1370, which typically includes client specific and confidential information.

[0220] The sender driven certificate enrollment system 1342 then generates a certificate digest 1347, as shown in Fig. 36. This certificate digest 1347 contains most of the information necessary to generate a digital certificate 1345 for the client 1370, including the client specific data 1348, and the type of certificate to generate 1349 (e.g. an X.509 certificate). In a preferred embodiment, the certificate digest 1347 is forwarded to a secure SDCE server 1358. The SDCE server 1358 then "contacts" the client 1370 seeking independent confirmation of the confidential information 1348. For example, in a preferred embodiment of the invention, the SDCE server 1358 forwards an e-mail message to the client 1370 with a unique, dynamically generated URL (uniform resource locator). The client 1370 can then "click" or access this URL through a standard web browser. Accessing the URL begins a direct interaction, or SDCE conversation 1368, between the client 1370 and the SDCE server 1358.

[0221] The client 1370 is typically asked to input one or more pieces of confidential information 1348 to the SDCE server 1358. In a preferred embodiment, the conversation takes place over a secure socket layer (SSL) channel between client 1370 and the SDCE server 1358, and utilizes HTML forms.

[0222] The SDCE server 1358 then attest whether the client 1370 is correct, by comparing input information to the stored client information 1348 within the stored certificate digest 1347. On a match, the SDCE server 1358 forwards the certificate digest 1347 over a secure channel to the recipient client's desktop 1372, and also distributes software to the recipient client 1370, which uses the certificate digest 1347 to generate a key pair 1332, 1340 on the recipient system. In the preferred embodiment of the invention, this software is simply a Java applet, transparently forwarded to the recipient 1370 through the browser. The generated private key 1332 is stored on the recipient system 1370, preferably using the PKCS12 format. The public key 1332 is forwarded back to the SDCE server 1358, which typically registers both the public and client information as the digital certificate 1345 on a certificate server 1388, such as an LDAP or an Entrust certificate management server (of Entrust, Inc., Ottawa, Canada).

[0223] The sender (e.g. the attorney) 1352, can now access the stored public key 1332 for the intended recipient client 1370, encrypt the document 1312 intended for the recipient client 1370 with the public key 1332, and then send the encrypted document 1336 to the client 1370. The client 1370, in turn, decrypts 1338 the encrypted document 1336 with [the public key and] the corresponding private key 1340, which is now resident on the private recipient system 1370.

[0224] Fig. 37 shows the first stage 1350 of the sender driven certificate enrollment system 1342. A sender

[0235] SDCE Server Software. The SDCE Server software, in a preferred embodiment of the invention, includes a HTTP Web Server with a customized filter to intercept and redirect all HTTP requests, a e-mail server to forward notifications on to an intended recipient 1370, and the basic software and logic to query a database server, to generate a certificate digest 1347 (as described above), and to interact with all other components of the system.

[0236] The Web server is a primary interface between the SDCE server 1358 and the intended recipient 1370 of a document 1312, in which the SDCE server 1358 assists in the construction of a digital certificate 1345.

[0237] In a preferred embodiment of the invention, the SDCE server software initiates an attestation conversation 1366 (Fig. 38) with the intended recipient 1370, by dynamically generating a private URL. The private URL contains a key to uniquely identify the recipient 1370, and then forwards this "key" to the recipient over a standard e-mail notification. When the recipient 1370 accesses this "key" (which in fact is a private URL), the SDCE server 1358 associates the key with a given certificate digest 1347, and then through the Web interface, conducts the attestation conversation 1366, to verify that the given recipient 1370 matches the parameters of the certificate digest 1347.

[0238] Recipient Client Software. The sender driven certificate enrollment system 1342 creates a public/private key pair from a certificate digest 1347, which is forwarded from the SDCE server 1358 to the recipient system 1370. Client software on the recipient computer takes the certificate digest 1347, constructs the public/private key pair 1332, 1340 on the recipient desktop 1372, stores these keys 1332, 1340 on the recipient system 1370, and then forwards the public key 1332 to the SDCE server 1358.

[0239] In a preferred embodiment, the recipient client software is a Java applet, which is transparently and dynamically downloaded via a web browser, in which the recipient simply accesses an URL, as described above.

[0240] Certificate Server. The invention makes use of basic digital certificate management. The certificate server 1388 includes query ability, which determines if a digital certificate exists for a recipient given a specific user profile (*e.g.* an e-mail address and identifier). The certificate server 1388 also includes update ability, which allows a programmatic interface to add a new certificate to the server's database. In preferred embodiments, LDAP, X.500, or proprietary certificate servers such as a Entrust server can be used as certificate servers 1388.

[0241] Database Server. In a preferred embodiment of the invention, the SDCE server 1358 queries a database 1346 containing recipient information to construct a certificate digest 1347. In a basic embodiment, the sender's desktop 1354 can query an internal database 1346, or the sender's desktop 1354 can simply load information directly from the desktop 1354. The preferred database query provided by a SDCE server 1358 supports more scalability and extensibility.

[0242] In addition to the basic design for the invention, there remains situations wherein no recipient data 1348 exists which is readily accessible from the senders system 1352, either directly from the desktop 1354 or via a database query. In this case, the sender driven enrollment system 1342 still retains value. While the certificate digest 1347 contains limited information 1348, the level of attestation is also limited. However, basic attestation can still take place, and the system 1342 still simplifies the process of generating a basic digital certificate 1345 for the recipient 1370. In this case, the system behaves exactly as designed, with the exception being a more simplistic conversation 1366 and certificate digest 1347.

[0243] Fig. 41 is flow chart 1302 that describes the basic decision tree behind the sender driven certificate enrollment system 1342.

[0244] At step 102, the sender 1352 queries the certificate server 1388 for the public key 1332 of an intended recipient 1370 for a document 1312. If the public key 1332 exists, the document 1312 is encrypted with the public key 1332, and is sent to the recipient 1370, at step 104. If the public key 1332 doesn't exist, the sender queries the SDCE Server 1358 for a certificate digest 1347 for the intended recipient 1370, at step 1356.

[0245] The SDCE server 1358 then queries the database 1346 for information 1348 regarding the intended recipient 1370, at step 1360. If the information exists and is already stored in the database 1346, the SDCE server 1358 generates a rich certificate digest for the client 1370, at step 1365. If no information 1348 exists and is stored in the database 1346, the SDCE server 1358 generates a simplified certificate digest 1347, at step 1364.

[0246] At step 1368, the SDCE server 1358 initiates an attestation conversation 1366 with the recipient 1370. If there is no match to the information 1348, the SDCE server 1358 notifies the sender 1352, at step 106, and there is no generation of a key pair 1332, 1340. If there is a match, a private/public key pair 1332, 1340 for the recipient 1370 is generated on the recipient system 1370, at step 1380. The key pair is then forwarded to the SDCE server 1358, at step 1382. At step 1388, the SDCE server registers the certificate for the intended recipient 1370 with a certificate server 1388. At step 1390, the SDCE server notifies' the sender 1352 of the digital certificate 1345. The sender 1352 can then encrypt the document 1312 with the generated public key 1332 of the intended recipient 1370, as shown in Fig. 3. When the encrypted document 1336 is sent to the recipient 1370, typically over a network 1344, the recipient 1370 can decrypt the encrypted document 1336, using the stored private key 1340, as shown in Fig. 4.

[0247] Although the sender driven certificate enroll-

an HTML interface on a computer desktop (12) for managing said dedicated server (22) via a Web browser.

13. The apparatus of any of Claims 10 to 12, further comprising a send client application (20) for delivering said at least one document (16) as a single package from said desktop (12) of a sending computer (14) over said electronic network (18) during a session.

14. The apparatus of Claim 13, said send client application (20) comprising:

an application window (32,140) for displaying a send client application interface said application window (32,140) comprising a tool bar (34) for accessing main functions of said send client application (20), a package manager for listing all document activities initiated during a send client application session, and a menu listing operational commands for said send client application;
a package window (78,170) for specifying the parameters of said document delivery; and
a storage module for configurably storing said document delivery parameters, wherein said document delivery is initiated using said stored document delivery parameters.

15. The apparatus of any of Claims 10 to 14, further comprising a security framework for restricting access to said apparatus (10) and/or said document (16).

16. A method for document management and delivery on an electronic network (18) comprising the steps of:

delivering at least one document (16) as a single package from a sending computer (14) to a dedicated server (22,505) over an electronic network (18) during a session (500) using a send client application (20);
storing said at least one document (16,515) from said sending computer (14) on said dedicated server (22,505);
forwarding an electronic message to a receiving device (24,26,28,530) from said dedicated server (22,505); and
downloading said at least one stored document (535) from said dedicated server (22,505) using a receive client application (30) on said receiving device (24,26,28,530), in response to the electronic message.

17. The method of Claim 16, further comprising the step of:

said sending computer desktop (12) displaying an application window (32,140) with a send client application interface having a tool bar for accessing main functions of said send client application (20), a package manager for listing all document activities initiated during said session (500), and a menu listing operational commands for said send client application (20).

18. The method of Claim 17, further comprising the step of:

specifying the parameters of said document delivery in a packaging window (78,170).

19. The method of Claim 18, comprising the step of:

configurably storing, in a storage module, said specified document delivery parameters, wherein said document delivery is initiated using said stored document delivery parameters.

20. The method of any of Claims 16 to 19, further comprising the step of:

providing a security framework for restricting access to said system, said security framework supporting at least one of authentication layers, secure socket layers, password protection, private key encryption, public key encryption, and certificate authentication.

21. The method of any of Claims 16 to 20, further comprising the step of:

initiating said document delivery from the contents of an address book of a supported application on said sending computer (14).

22. The method of any of Claims 16 to 21, comprising the step of:

displaying a Configuration User Interface application window (140) for managing said dedicated server (22,505) on a computer desktop (12), said configuration user interface application window (140) having a main tool bar for accessing main functions of said configuration user interface, a secondary tool bar for accessing functions within said main functions, a workspace for displaying an interactive interface to an accessed function, and a menu listing operational commands for said configuration user interface.

23. An apparatus for generating a digital certificate (1345) for a recipient (1370) by a sender (1352),

step of comparing said gathered information with said queried, stored recipient information (1348) is performed by a server (1358,1362,1388).

41. The method of any of Claims 34 to 40, further comprising the step of:

generating a certificate digest (1347) comprising said stored recipient information (1348) and sender selectable options (1349) for said digital certificate (1345).

Fig. 3

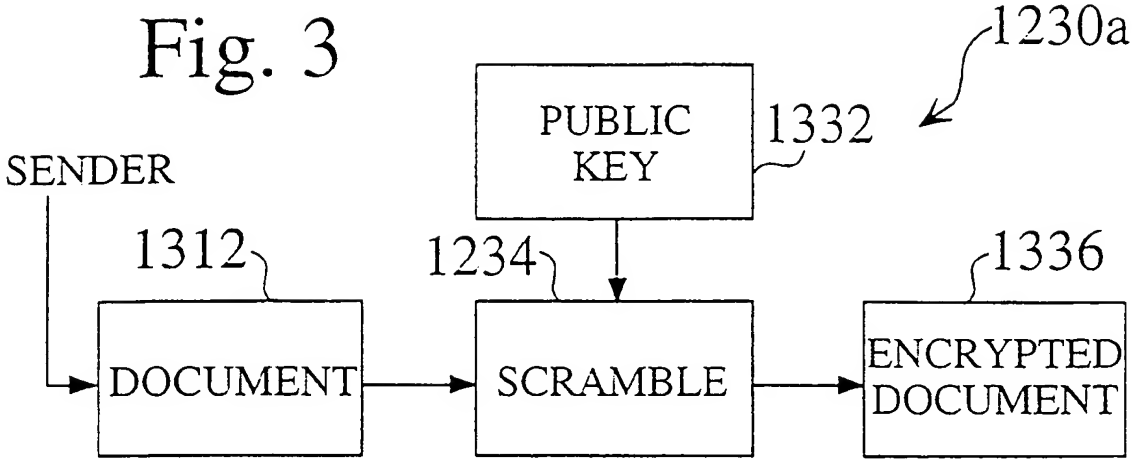
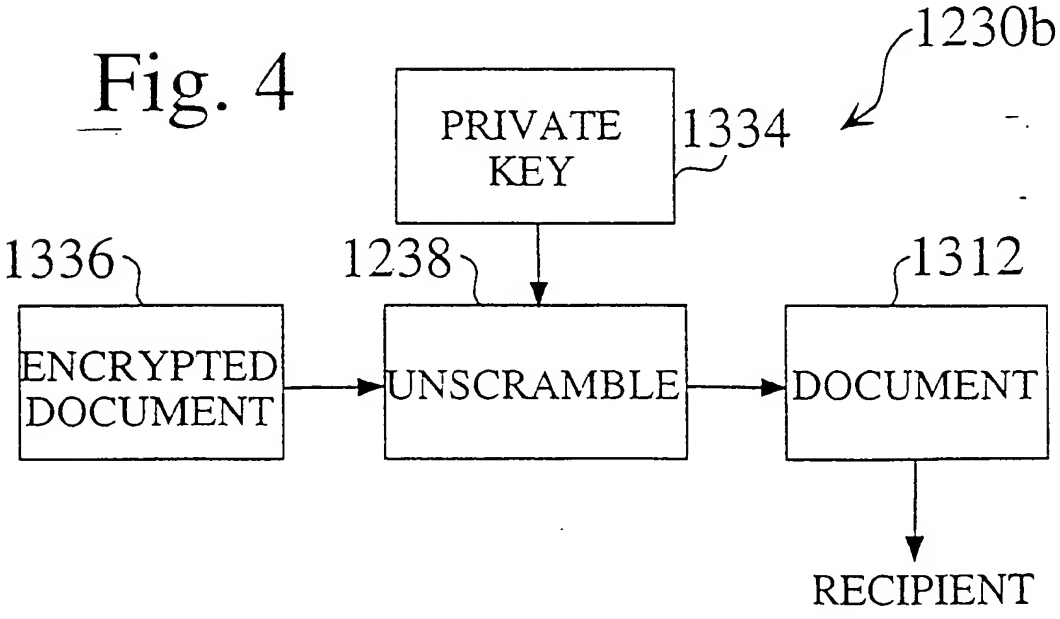

1230a
PUBLIC KEY
1332
SENDER
1312
1234
1336
DOCUMENT
SCRAMBLE
ENCRYPTED DOCUMENT

Fig. 4


1230b
PRIVATE KEY
1334
1336
1238
1312
ENCRYPTED DOCUMENT
UNSCRAMBLE
DOCUMENT
RECIPIENT

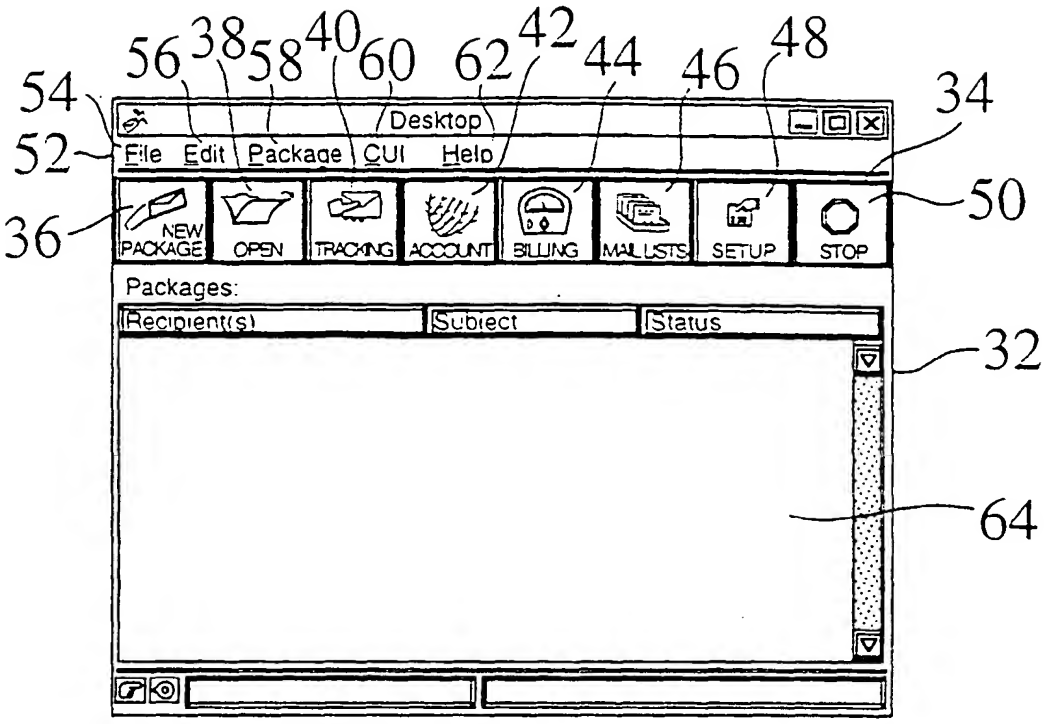

56
38
58
40
60
62
42
44
46
48
54
34
Desktop
52
File Edit Package CUI Help
36
NEW PACKAGE
OPEN
TRACKING
ACCOUNT
BILLING
MAIL LISTS
SETUP
STOP
50
Packages:
Recipient(s)
Subject
Status
32
64

Fig. 6

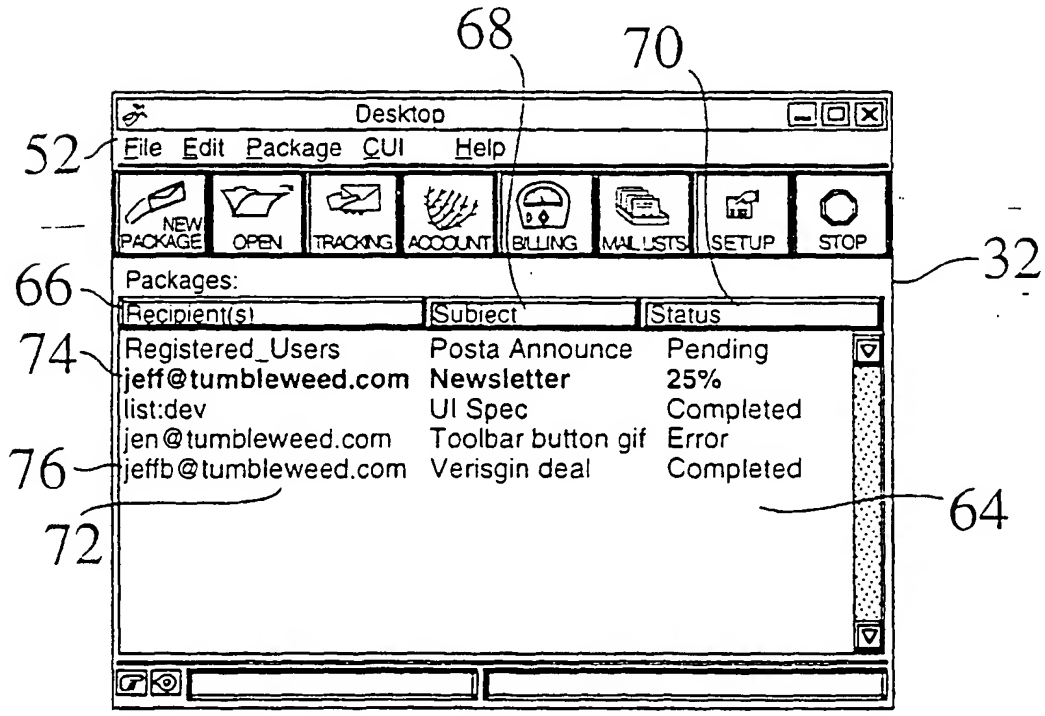

68
70
Desktop
52
File Edit Package CUI Help
NEW PACKAGE
OPEN
TRACKING
ACCOUNT
BILLING
MAIL LISTS
SETUP
STOP
32
66
Packages:
Recipient(s)
Subject
Status
74
Registered_Users
Posta Announce
Pending
jeff@tumbleweed.com
Newsletter
25%
list:dev
UI Spec
Completed
jen@tumbleweed.com
Toolbar button gif
Error
76
jeffb@tumbleweed.com
Verisgin deal
Completed
72
64

Fig. 7

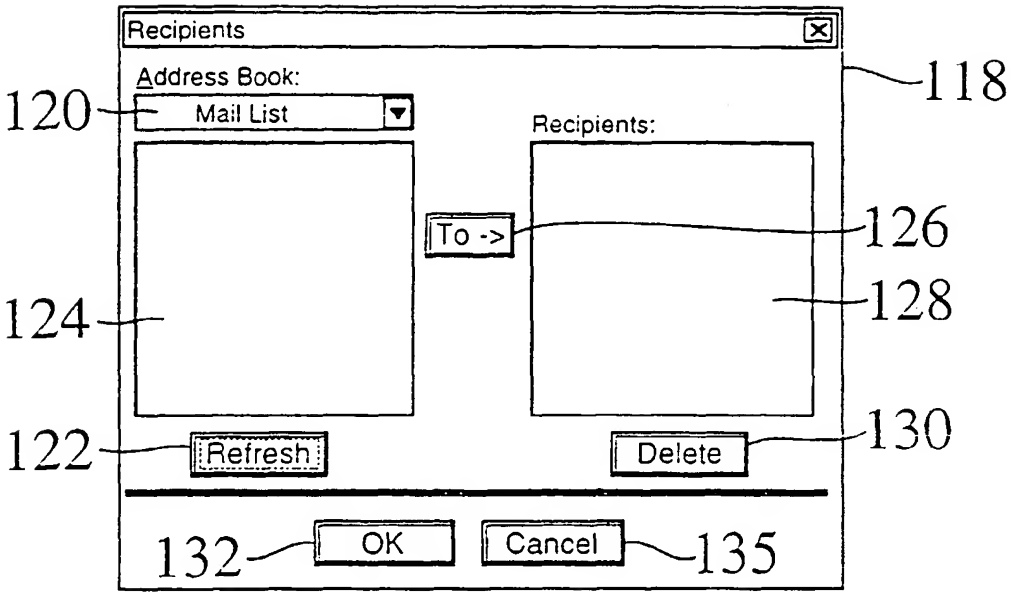

Recipients
Address Book:
Mail List
Recipients:
To ->
Refresh
Delete
OK
Cancel
118
120
122
124
126
128
130
132
135

Fig. 9

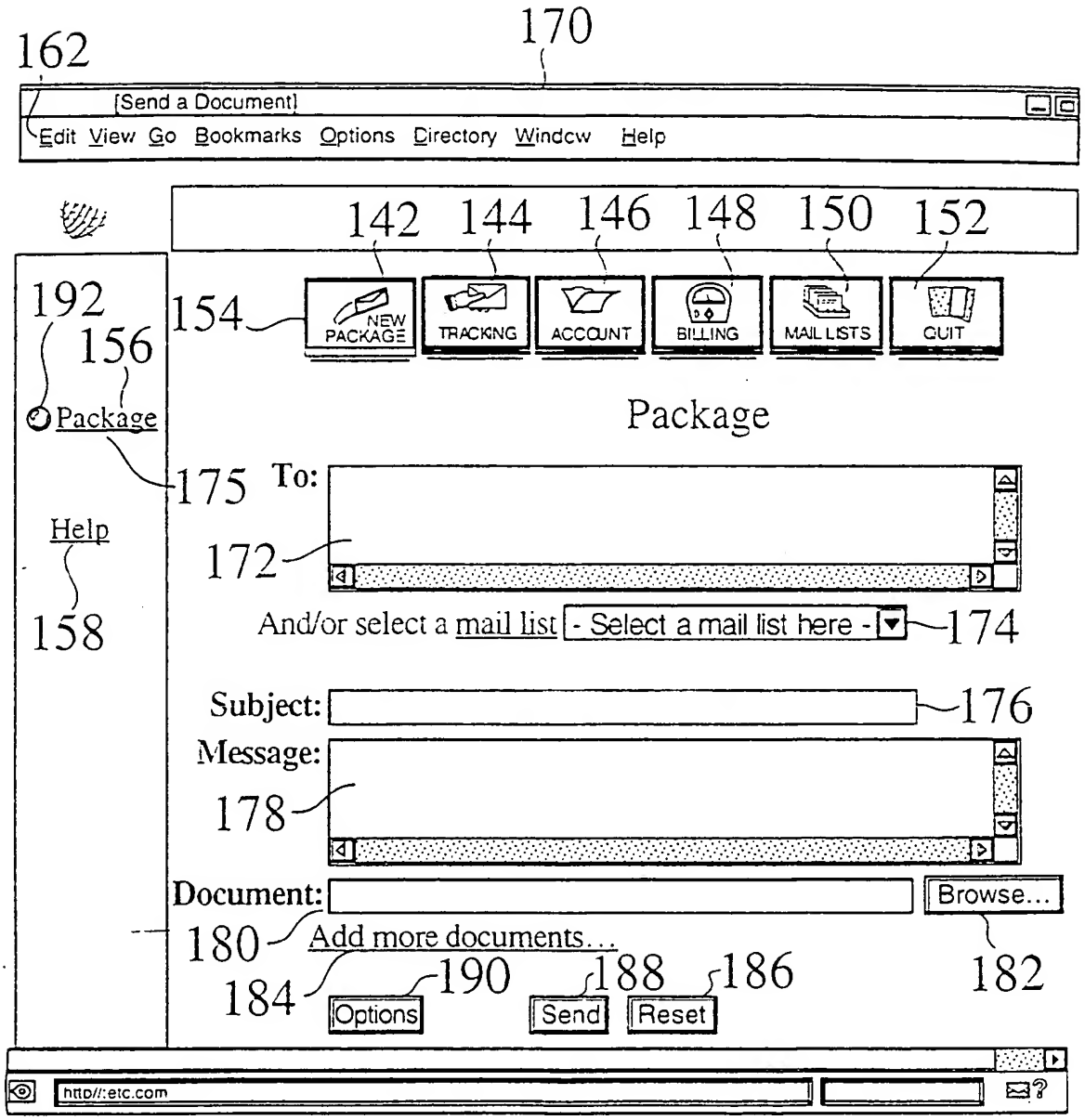

162
170
[Send a Document]
Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
192
156
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
Package
Package
175
To:
Help
172
158
And/or select a mail list
- Select a mail list here -
174
Subject:
176
Message:
178
Document:
Browse...
180
Add more documents...
184
190
188
186
182
Options
Send
Reset
http//:etc.com

Fig. 11

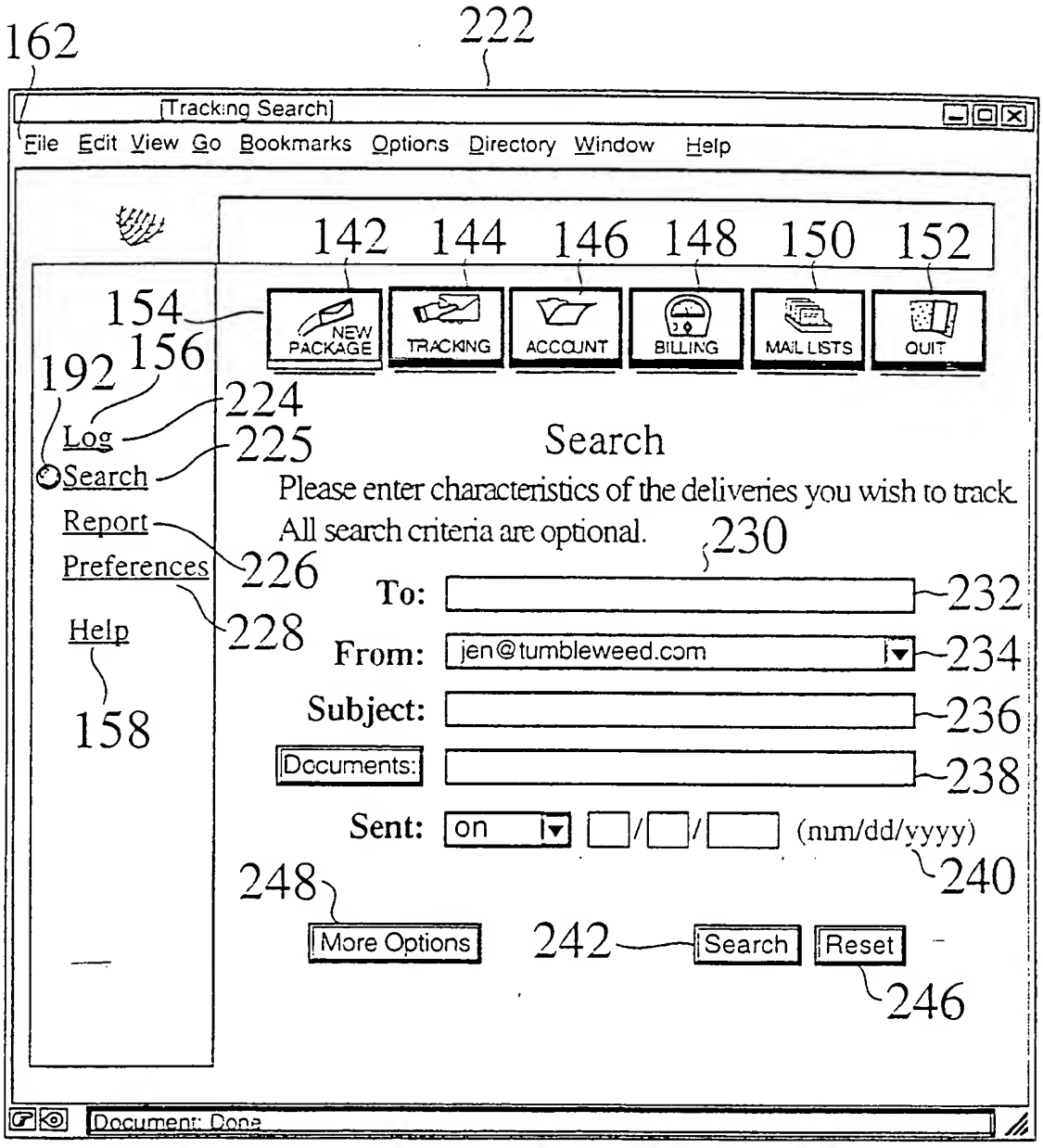

162
222
[Tracking Search]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
192 156
224
Log
225
Search
Report
Preferences
226
228
Help
158
Search
Please enter characteristics of the deliveries you wish to track.
All search criteria are optional.
230
To:
232
From:
jen@tumbleweed.com
234
Subject:
236
Documents:
238
Sent:
on
(mm/dd/yyyy)
240
248
More Options
242
Search
Reset
246
Document: Done

Fig. 13

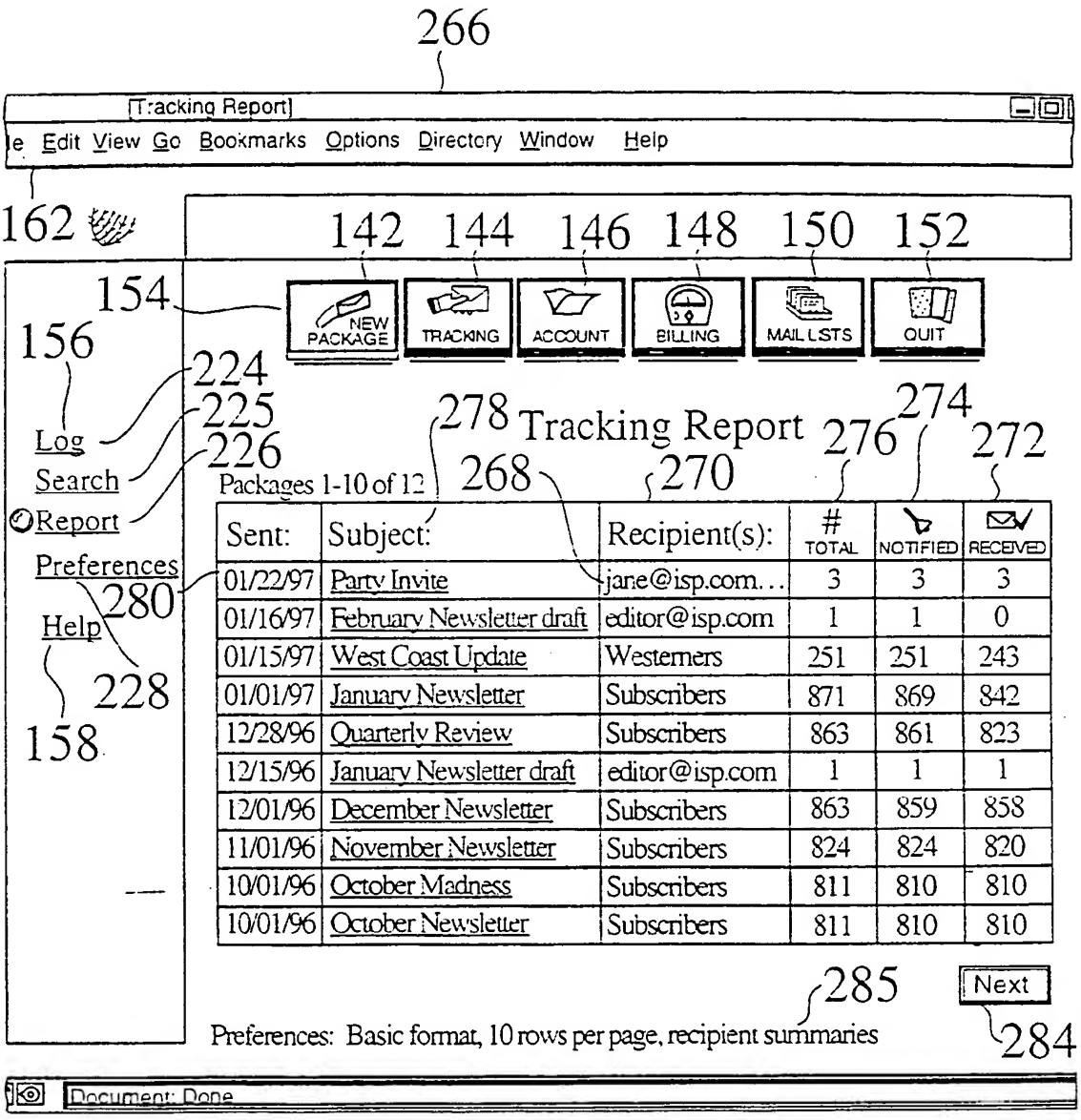

266
[Tracking Report]
le Edit View Go Bookmarks Options Directory Window Help
162
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LSTS
QUIT
156
224
225
226
Log
Search
Report
Preferences
280
Help
228
158
278
Tracking Report
276
274
272
268
270
Packages 1-10 of 12
Sent:
Subject:
Recipient(s):
TOTAL
NOTIFIED
RECEIVED
01/22/97 Party Invite jane@isp.com... 3 3 3
01/16/97 February Newsletter draft editor@isp.com 1 1 0
01/15/97 West Coast Update Westerners 251 251 243
01/01/97 January Newsletter Subscribers 871 869 842
12/28/96 Quarterly Review Subscribers 863 861 823
12/15/96 January Newsletter draft editor@isp.com 1 1 1
12/01/96 December Newsletter Subscribers 863 859 858
11/01/96 November Newsletter Subscribers 824 824 820
10/01/96 October Madness Subscribers 811 810 810
10/01/96 October Newsletter Subscribers 811 810 810
285
Next
284
Preferences: Basic format, 10 rows per page, recipient summaries
Document: Done

Fig. 15

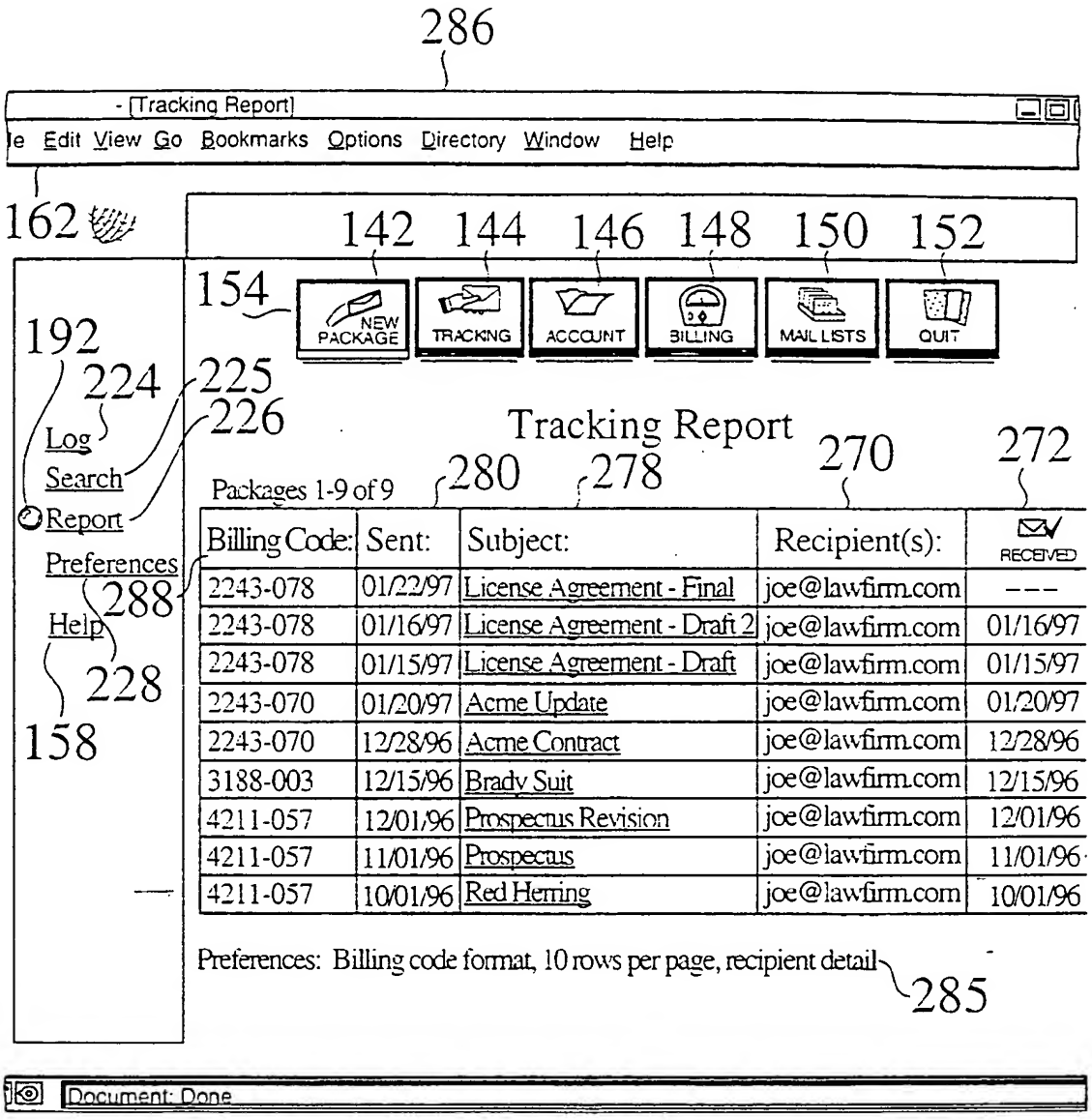

286
- [Tracking Report]
le Edit View Go Bookmarks Options Directory Window Help
162
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
192
224
225
226
Log
Search
Report
Preferences
288
Help
228
158
Tracking Report
270
272
Packages 1-9 of 9
280
278
Billing Code:
Sent:
Subject:
Recipient(s):
RECEIVED
2243-078 01/22/97 License Agreement - Final joe@lawfirm.com ---
2243-078 01/16/97 License Agreement - Draft 2 joe@lawfirm.com 01/16/97
2243-078 01/15/97 License Agreement - Draft joe@lawfirm.com 01/15/97
2243-070 01/20/97 Acme Update joe@lawfirm.com 01/20/97
2243-070 12/28/96 Acme Contract joe@lawfirm.com 12/28/96
3188-003 12/15/96 Brady Suit joe@lawfirm.com 12/15/96
4211-057 12/01/96 Prospectus Revision joe@lawfirm.com 12/01/96
4211-057 11/01/96 Prospectus joe@lawfirm.com 11/01/96
4211-057 10/01/96 Red Herring joe@lawfirm.com 10/01/96
Preferences: Billing code format, 10 rows per page, recipient detail
285
Document: Done

Fig. 17

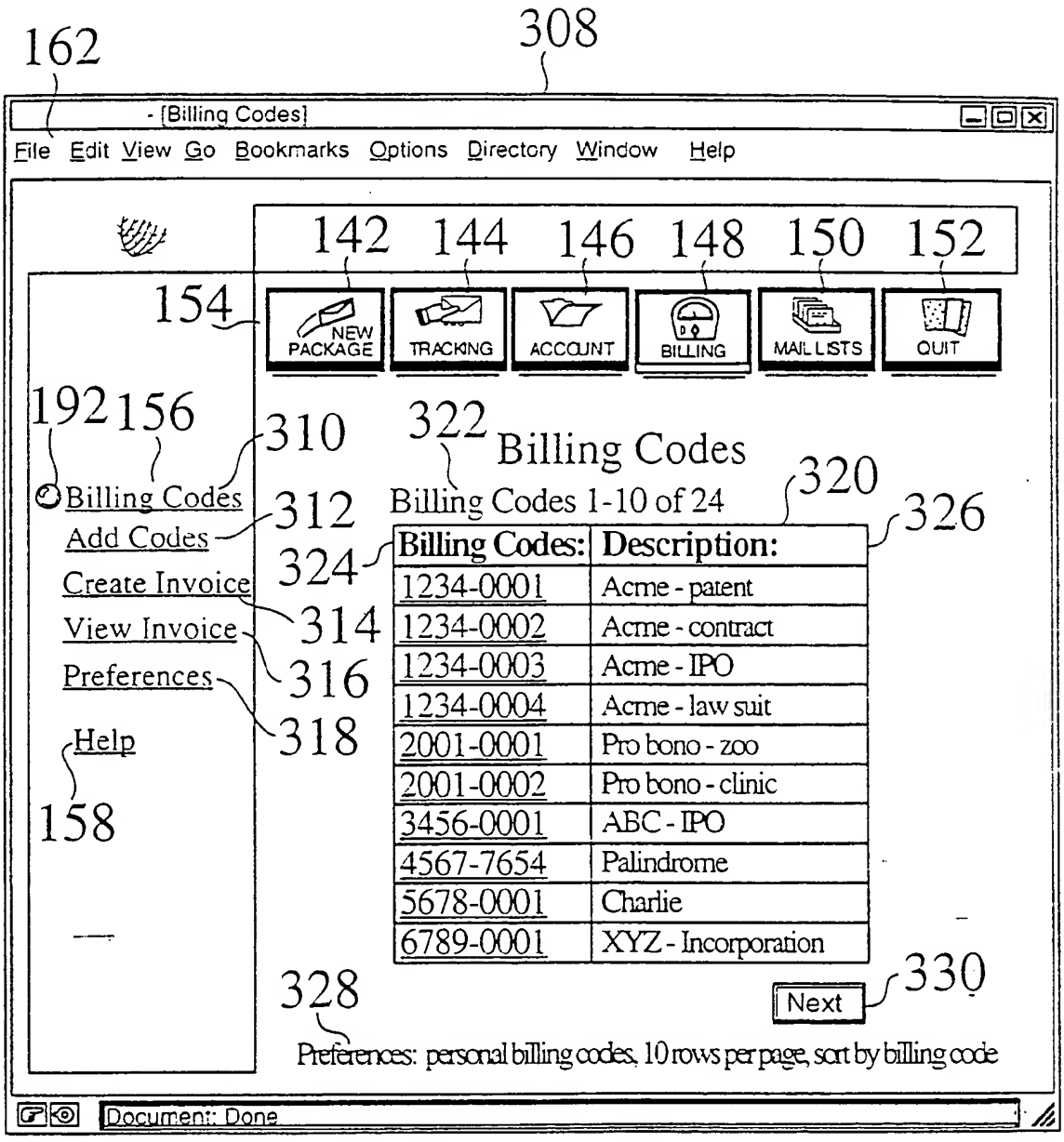

162
308
- [Billing Codes]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
192 156
310
322
Billing Codes
Billing Codes
Billing Codes 1-10 of 24
320
326
Add Codes
312
324
Billing Codes: | Description:
Create Invoice
314
1234-0001 | Acme - patent
View Invoice
316
1234-0002 | Acme - contract
1234-0003 | Acme - IPO
Preferences
318
1234-0004 | Acme - law suit
2001-0001 | Pro bono - zoo
Help
2001-0002 | Pro bono - clinic
158
3456-0001 | ABC - IPO
4567-7654 | Palindrome
5678-0001 | Charlie
6789-0001 | XYZ - Incorporation
328
330
Next
Preferences: personal billing codes, 10 rows per page, sort by billing code
Document: Done

Fig. 19

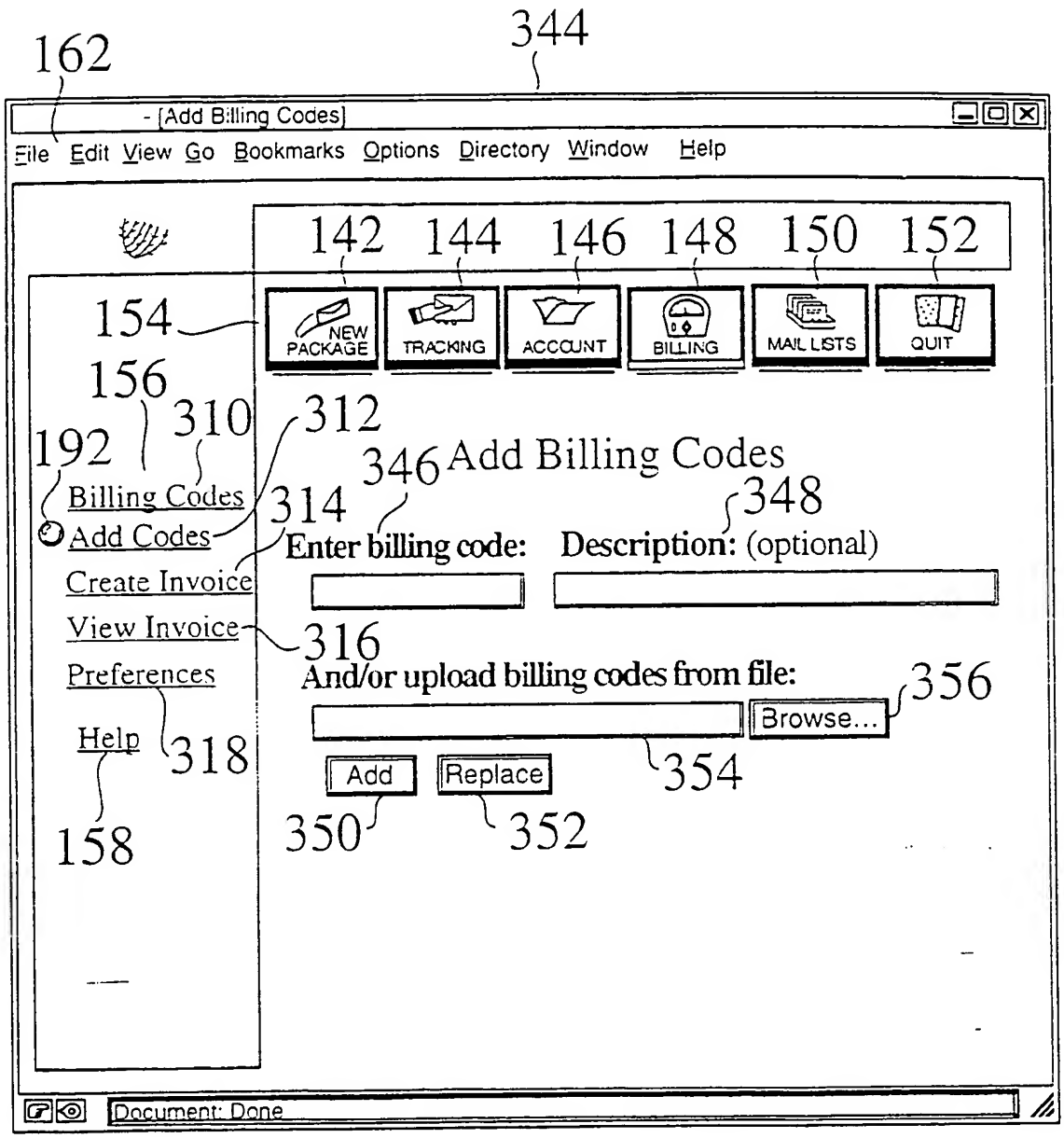

162
344
- [Add Billing Codes]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
154
156
310
312
192
346
Add Billing Codes
Billing Codes
314
348
Add Codes
Enter billing code:
Description: (optional)
Create Invoice
View Invoice
316
Preferences
And/or upload billing codes from file:
356
Browse...
Help
318
354
Add
Replace
158
350
352
Document: Done

Fig. 21

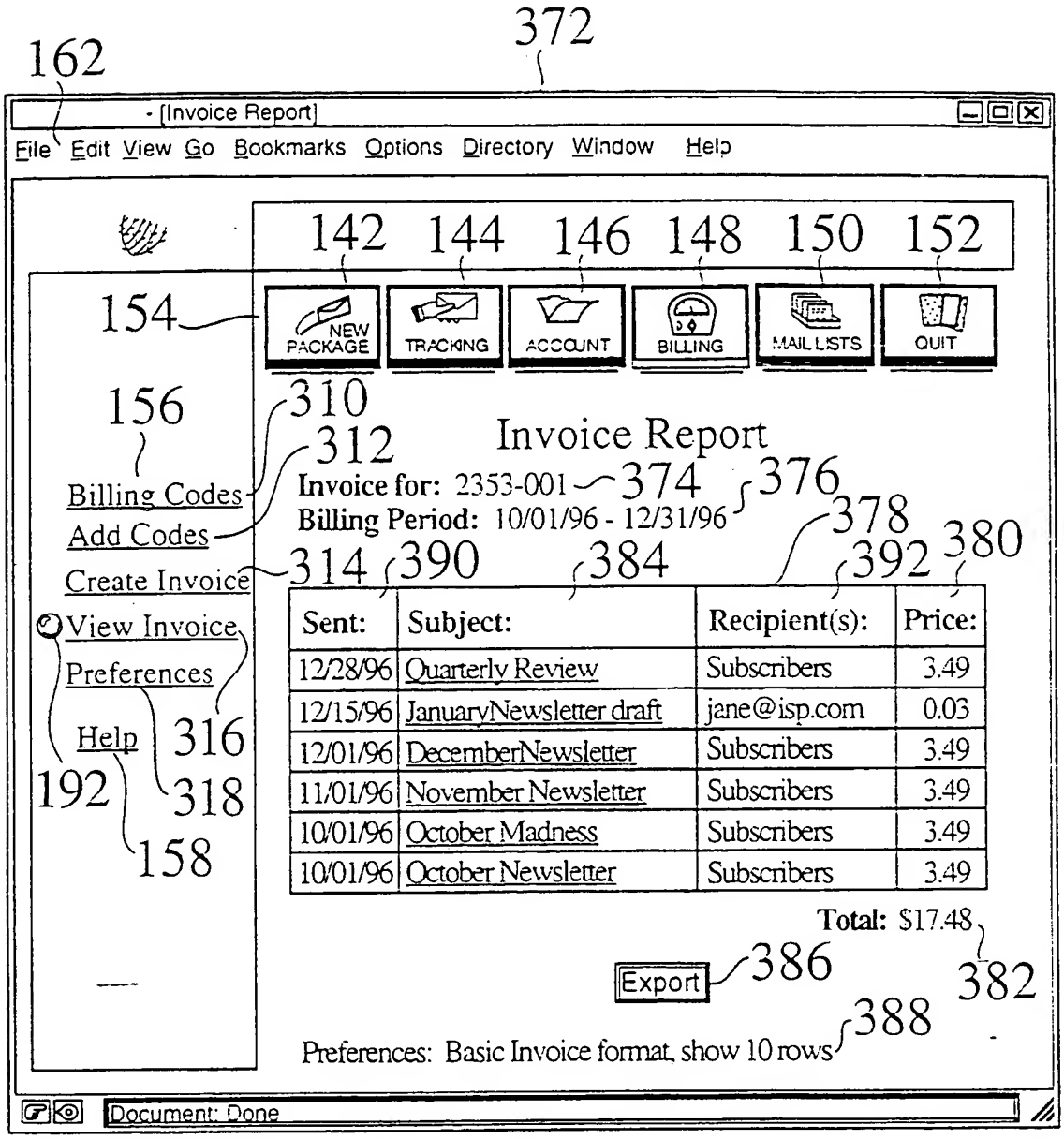

162
372
- [Invoice Report]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
156
310
312
Billing Codes
Add Codes
Create Invoice
View Invoice
Preferences
Help
192
158
316
318
Invoice Report
Invoice for: 2353-001
374
376
Billing Period: 10/01/96 - 12/31/96
378
314
390
384
392
380
Sent: | Subject: | Recipient(s): | Price:
12/28/96 | Quarterly Review | Subscribers | 3.49
12/15/96 | JanuaryNewsletter draft | jane@isp.com | 0.03
12/01/96 | DecemberNewsletter | Subscribers | 3.49
11/01/96 | November Newsletter | Subscribers | 3.49
10/01/96 | October Madness | Subscribers | 3.49
10/01/96 | October Newsletter | Subscribers | 3.49
Total: $17.48
382
Export
386
388
Preferences: Basic Invoice format, show 10 rows
Document: Done

Fig. 23

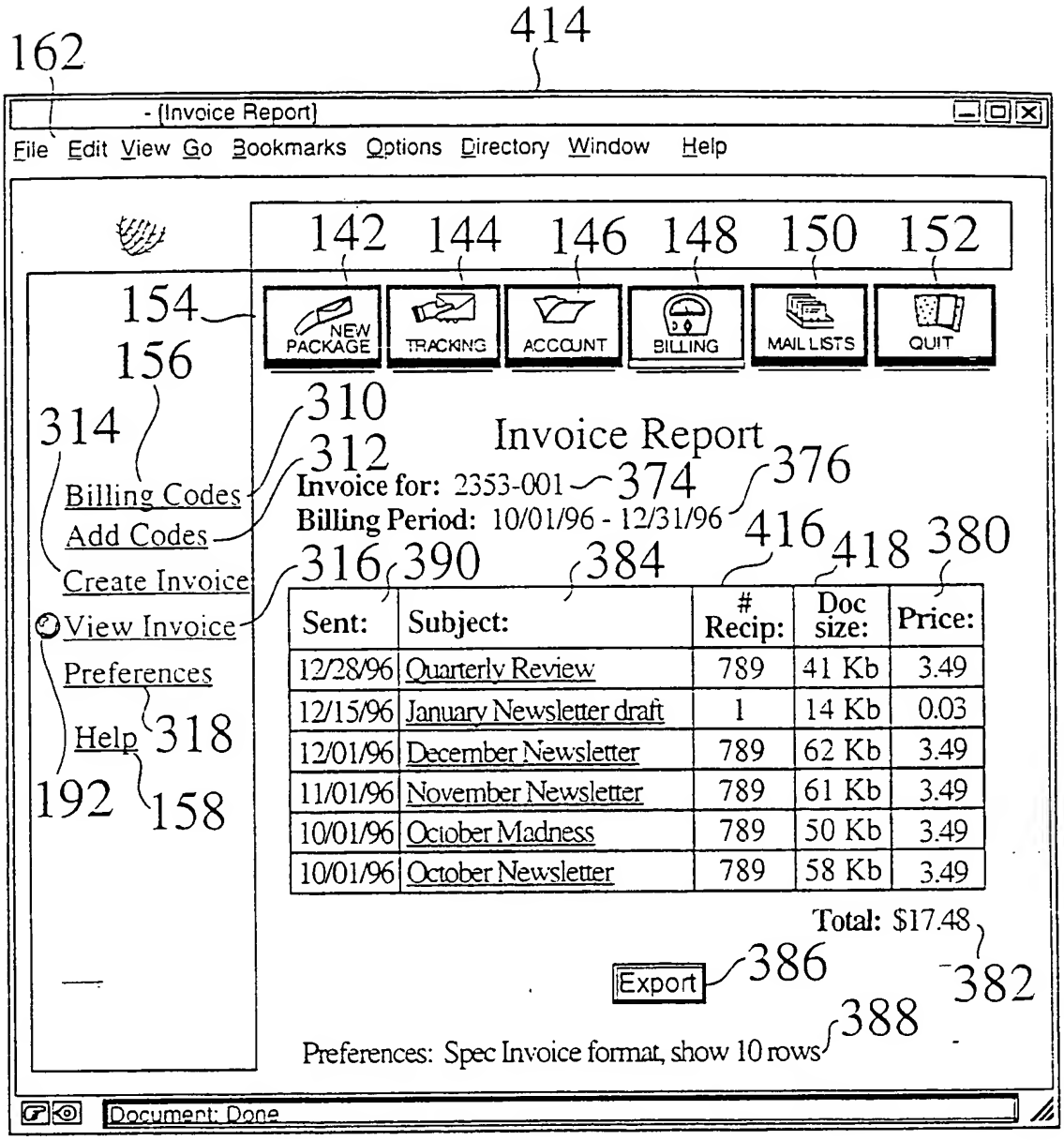

162
414
- (Invoice Report)
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
156
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
314
310
312
Billing Codes
Add Codes
Create Invoice
View Invoice
Preferences
Help
192
158
318
Invoice Report
Invoice for: 2353-001
374
376
Billing Period: 10/01/96 - 12/31/96
416
418
380
316
390
384
Sent:
Subject:
Recip:
Doc size:
Price:
12/28/96 Quarterly Review 789 41 Kb 3.49
12/15/96 January Newsletter draft 1 14 Kb 0.03
12/01/96 December Newsletter 789 62 Kb 3.49
11/01/96 November Newsletter 789 61 Kb 3.49
10/01/96 October Madness 789 50 Kb 3.49
10/01/96 October Newsletter 789 58 Kb 3.49
Total: $17.48
382
Export
386
388
Preferences: Spec Invoice format, show 10 rows
Document: Done

Fig. 25

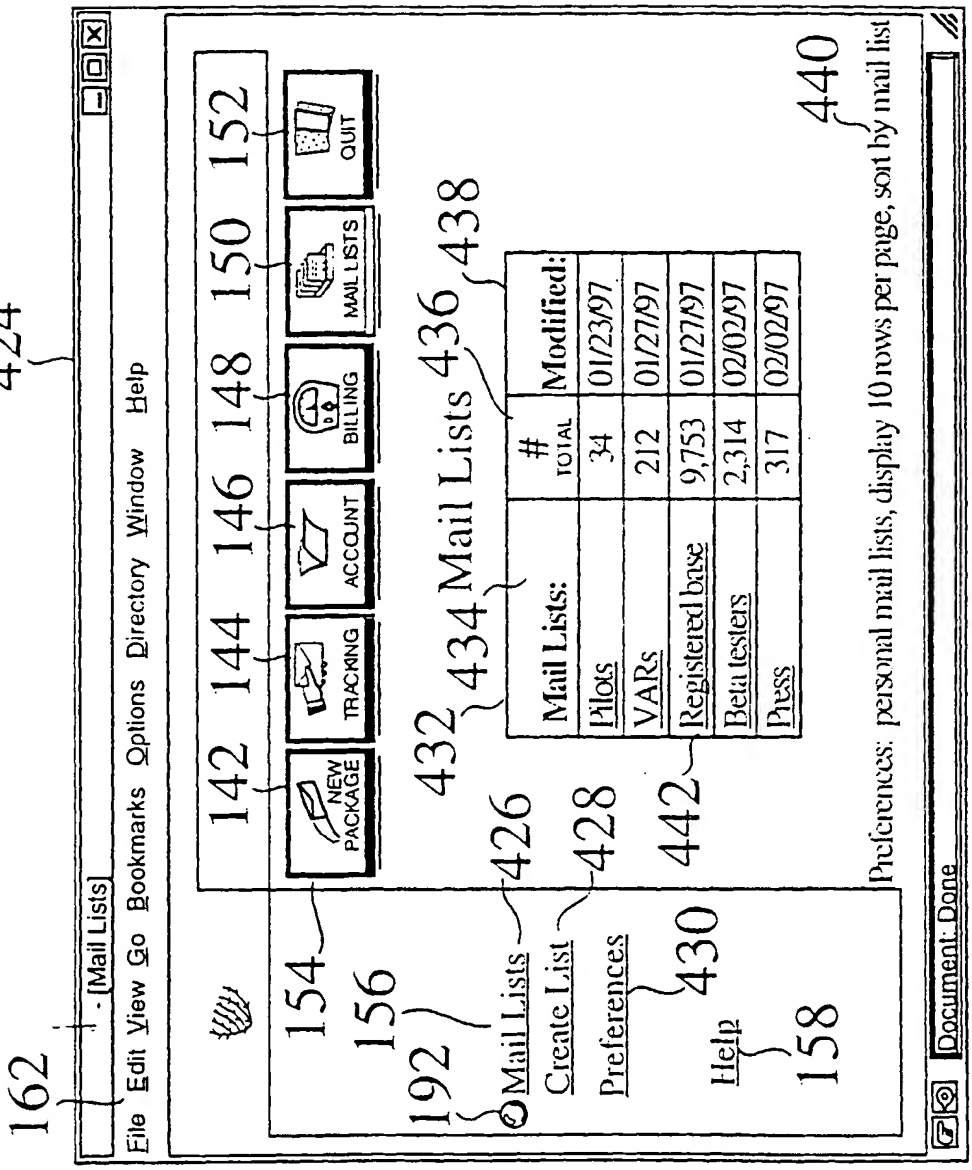

424
- [Mail Lists]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
154
156
192
Mail Lists
Create List
Preferences
Help
158
430
426
428
442
432
434 Mail Lists 436
438
Mail Lists:
TOTAL
Modified:
Pilots 34 01/23/97
VARs 212 01/27/97
Registered base 9,753 01/27/97
Beta testers 2,314 02/02/97
Press 317 02/02/97
440
Preferences: personal mail lists, display 10 rows per page, sort by mail list
Document: Done
162

Fig. 27

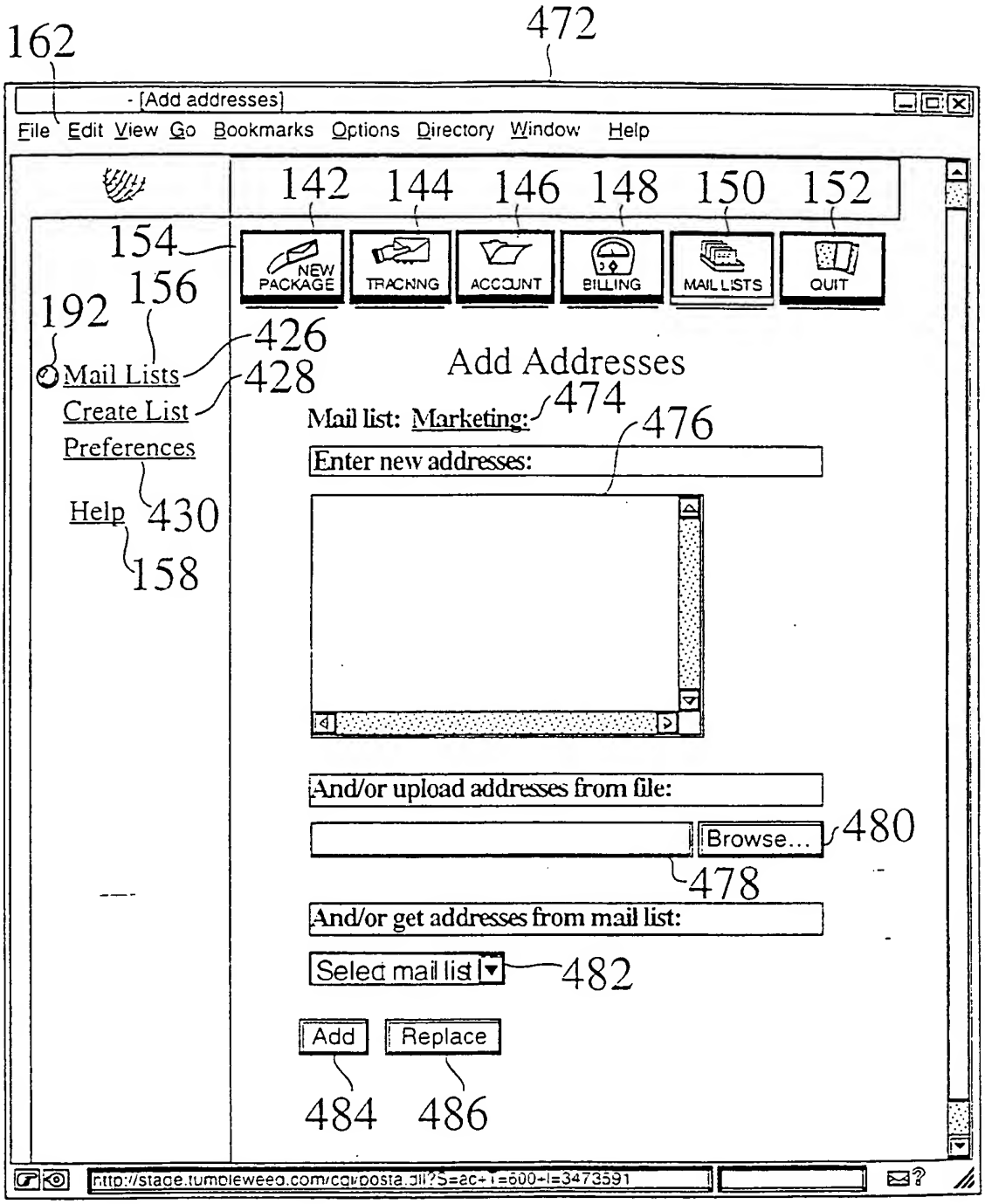

162
472
- [Add addresses]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
192
156
426
428
Mail Lists
Create List
Preferences
Help
430
158
Add Addresses
Mail list: Marketing:
474
476
Enter new addresses:
And/or upload addresses from file:
Browse...
480
478
And/or get addresses from mail list:
Select mail list
482
Add
Replace
484
486
http://stage.tumbleweed.com/cgi/posta.dll?S=ac+1=600+l=3473591

Fig. 29

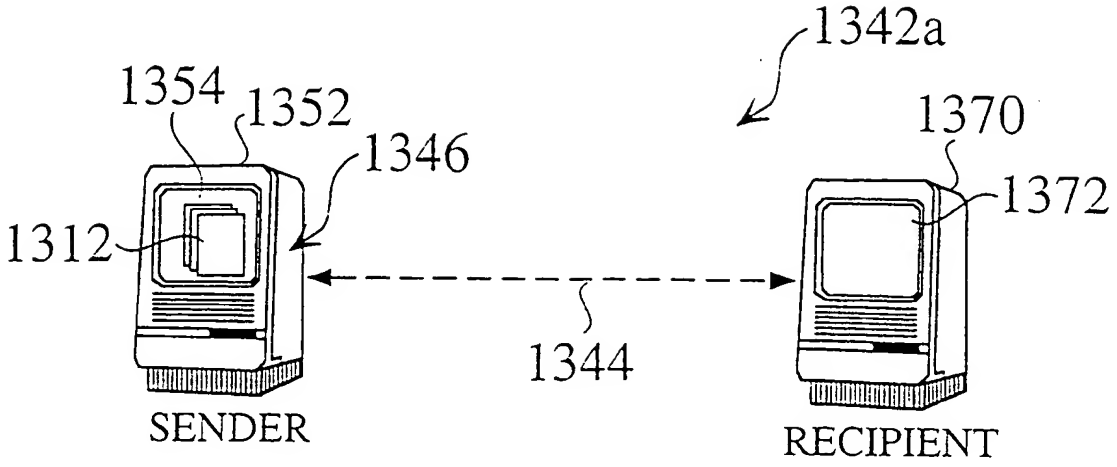

1342a
1354
1352
1346
1370
1372
1312
1344
SENDER
RECIPIENT

Fig. 31

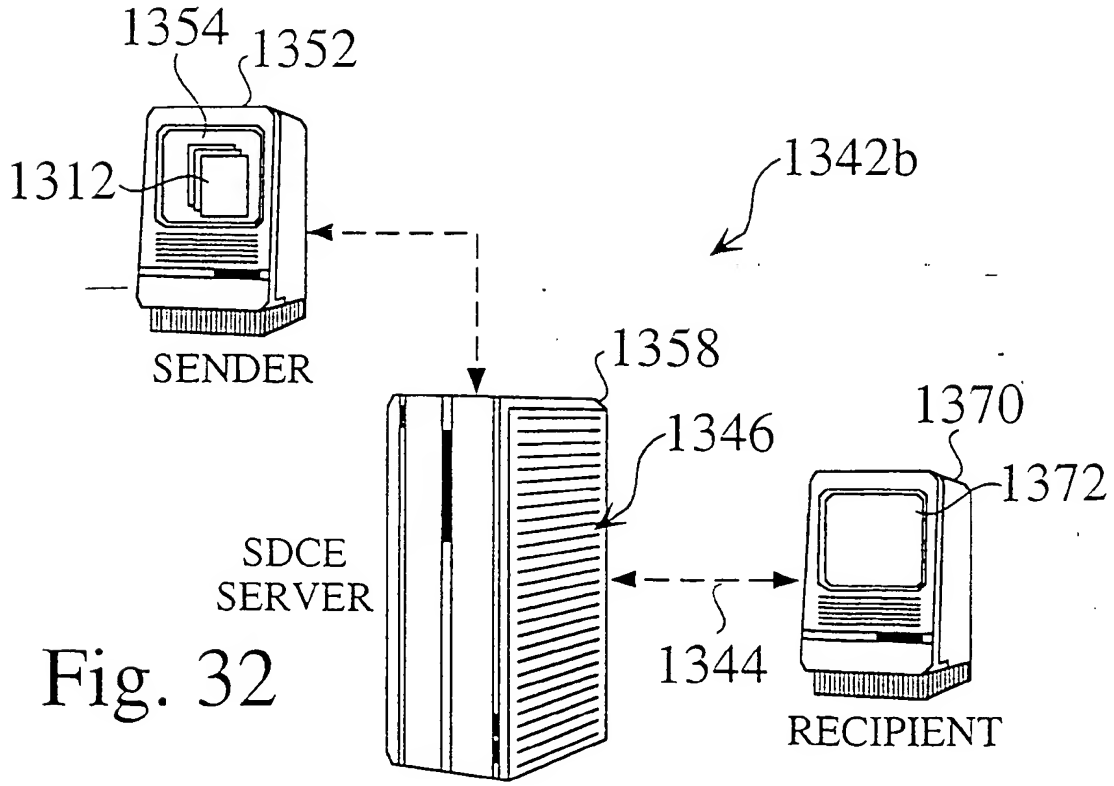

1354
1352
1342b
1312
SENDER
1358
1370
1346
1372
SDCE
SERVER
1344
RECIPIENT

Fig. 32

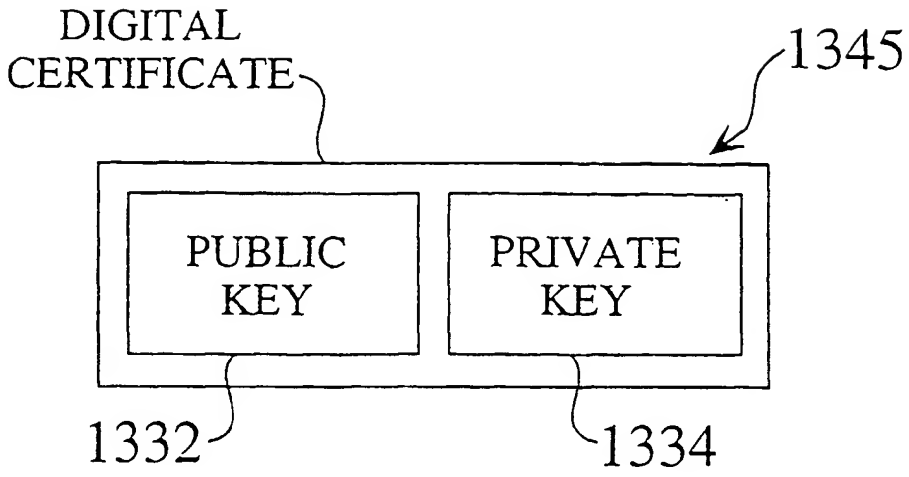

DIGITAL
CERTIFICATE
1345
PUBLIC
KEY
PRIVATE
KEY
1332
1334

Fig. 35

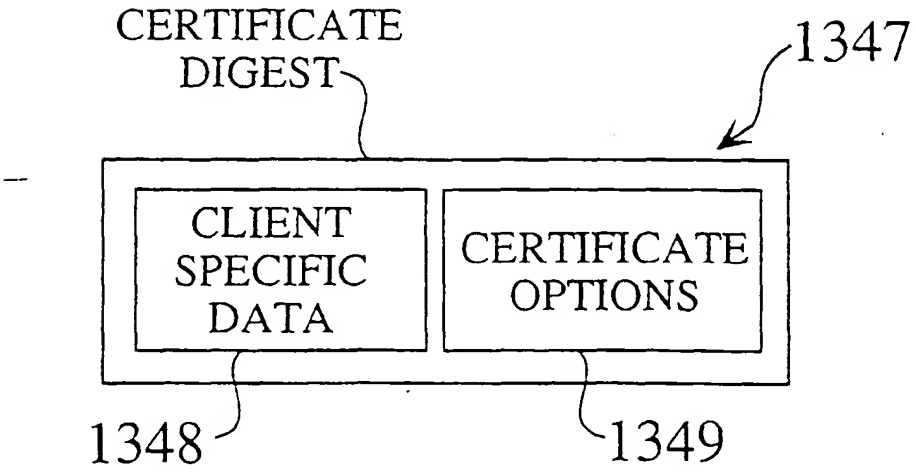

CERTIFICATE
DIGEST
1347
CLIENT
SPECIFIC
DATA
CERTIFICATE
OPTIONS
1348
1349

Fig. 36

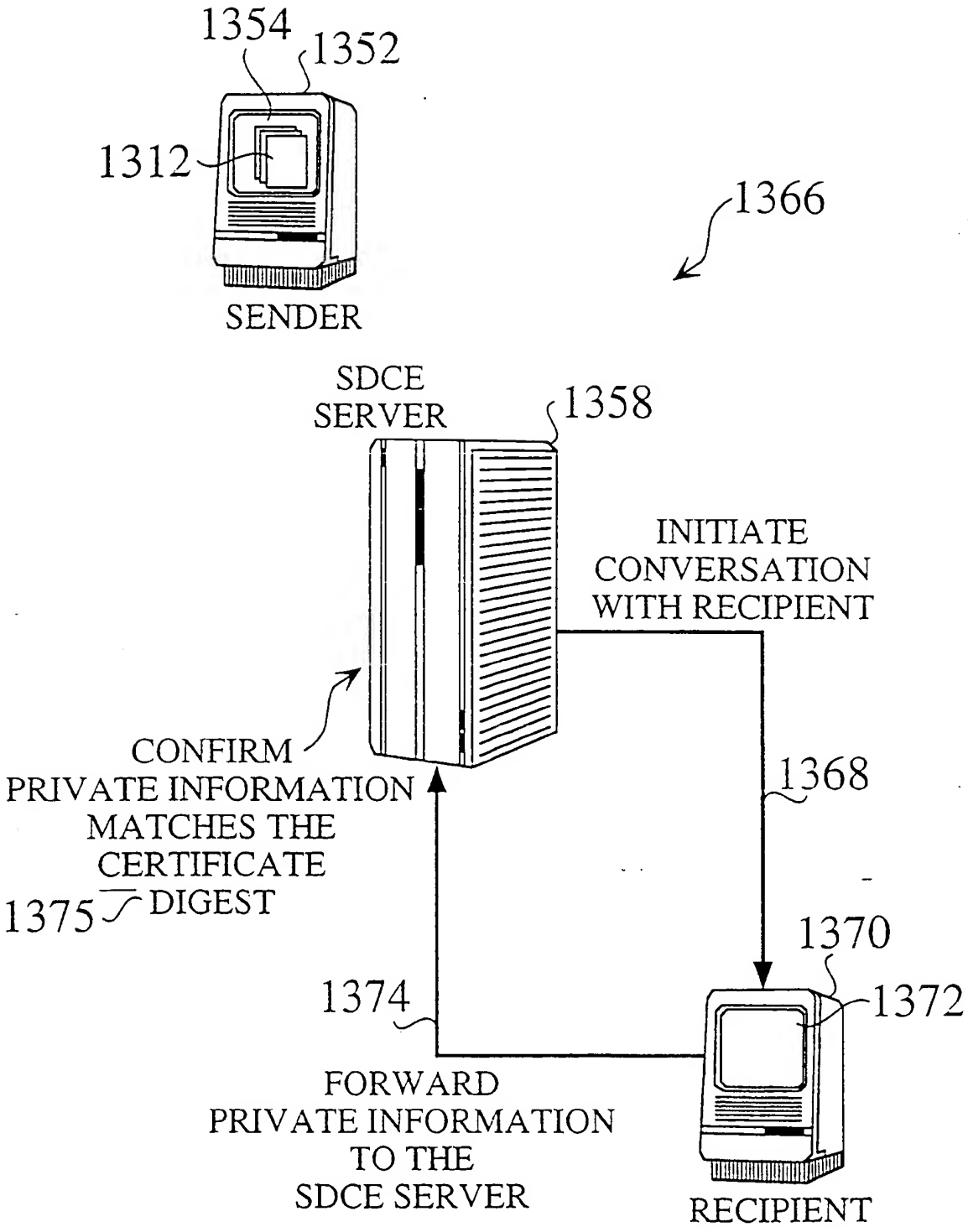

1354
1352
1312
1366
SENDER
SDCE
SERVER
1358
INITIATE
CONVERSATION
WITH RECIPIENT
CONFIRM
PRIVATE INFORMATION
MATCHES THE
CERTIFICATE
DIGEST
1375
1368
1370
1374
1372
FORWARD
PRIVATE INFORMATION
TO THE
SDCE SERVER
RECIPIENT

Fig. 38

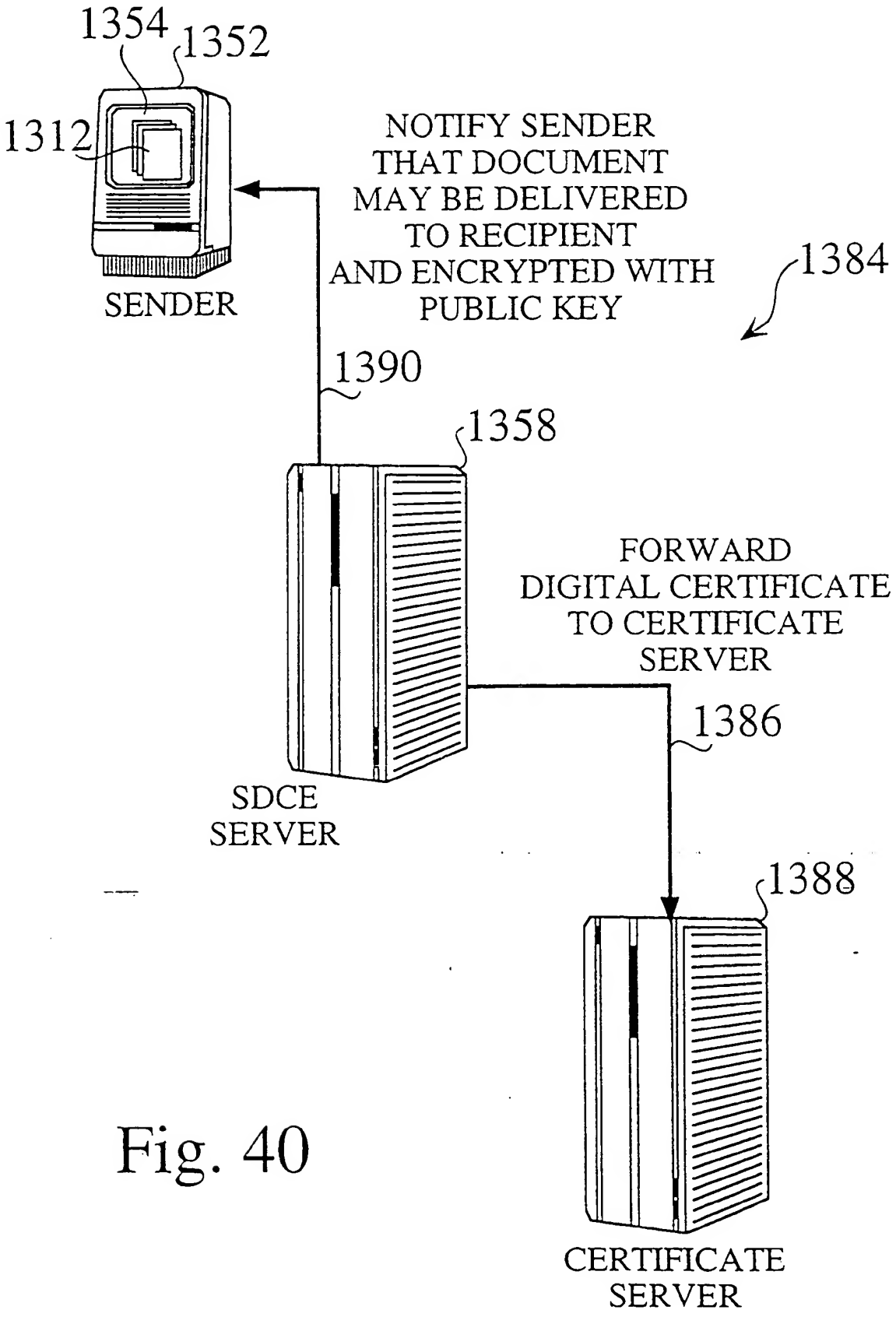

1354
1352
1312
SENDER
NOTIFY SENDER
THAT DOCUMENT
MAY BE DELIVERED
TO RECIPIENT
AND ENCRYPTED WITH
PUBLIC KEY
1384
1390
1358
FORWARD
DIGITAL CERTIFICATE
TO CERTIFICATE
SERVER
1386
SDCE
SERVER
1388
CERTIFICATE
SERVER

Fig. 40

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 907 120 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
24.03.2004 Bulletin 2004/13

(43) Date of publication A2:
07.04.1999 Bulletin 1999/14

(21) Application number: **98118486.4**

(22) Date of filing: **30.09.1998**

(51) Int Cl.[7]: **G06F 1/00**, H04L 9/32, H04L 29/06, H04L 12/58

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **02.10.1997 US 957986**
09.04.1998 US 57966

(71) Applicant: **Tumbleweed Software Corporation**
Redwood City, California 94063 (US)

(72) Inventors:
- **Smith, Jeffrey C.**
  Menlo Park, CA 94025 (US)
- **Bandini, Jean-Christophe**
  Cupertino, CA 95014 (US)
- **Shoup, Randy**
  San Francisco, CA (US)

(74) Representative:
Diehl, Hermann, Dr. Dipl.-Phys. et al
DIEHL, GLÄSER, HILTL & PARTNER
Patentanwälte
Augustenstrasse 46
80333 München (DE)

(54) Method amd apparatus for delivering documents over an electronic network

(57) A method and apparatus are provided for securely delivering documents over an electronic network (18) while preserving document formatting. The invention also provides security that restricts access to the system to an authorized user. A document is sent from a sending computer (14) to a dedicated server (22), using a send client application (20). A dedicated server (22) stores the document (16) and forwards an electronic notification to a receiving device (24,26,28). The stored document is downloaded from the dedicated server (22), using a receive client application (30), in response to the notification. The receive client application (30) permits the recipient to receive, view, print, and/or manipulate the document. A sender driven certificate enrollment system (1342) and methods of its use are also provided, in which a sender (1352) controls the generation of a digital certificate (1345) that is used to encrypt and send a document to a recipient (1370) in a secure manner.

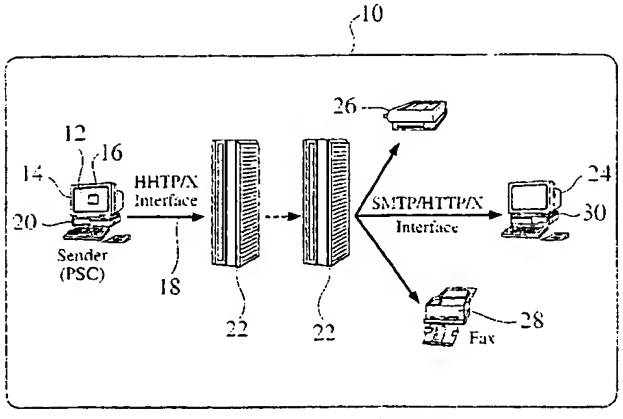


Fig. 5

EP 0 907 120 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 11 8486

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	WO 97/23082 A (AT & T CORP) 26 June 1997 (1997-06-26) * abstract * * page 1, line 7 - line 30 * * page 2, line 5 - page 3, line 19 * * page 3, line 26 - line 33 * * page 4, line 35 - page 8, line 18 * * figures 2-4 *	7	
Y	US 5 497 422 A (CALAMERA PABLO ET AL) 5 March 1996 (1996-03-05) * abstract * * column 1, line 57 - column 2, line 17 * * column 5, line 18 - column 6, line 51 * * column 8, line 11 - column 10, line 15 * * column 11, line 9 - column 13, line 55 * * column 18, line 65 - column 19, line 14 * * figures 1-13 * * claim 1 *	8,9,15	
A	WO 97/09682 A (ELONEX PLC) 13 March 1997 (1997-03-13) * abstract * * page 1, line 21 - page 4, line 2 * * page 5, line 8 - line 18 * * page 6, line 32 - page 9, line 24 * * figures 1-3 * * claims 1,2 *	1-22	

-/--

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	30 January 2004	Kopp, K

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 11 8486

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	EP 0 328 232 A (FISCHER ADDISON M) 16 August 1989 (1989-08-16) * page 2, line 4 - line 7 * * page 3, line 23 - page 4, line 35 * * page 5, line 6 - line 13 * * page 5, line 45 - page 7, line 20 * * page 8, line 1 - line 4 * * page 8, line 45 - page 9, line 17 * * figures 2-6 *	23-41	
A	LEVIEN R: "PROTECTING INTERNET E-MAIL FROM PRYING EYES" DATA COMMUNICATIONS, MCGRAW HILL. NEW YORK, US, vol. 25, no. 6, 1 May 1996 (1996-05-01), pages 117-118,120,122, XP000587586 ISSN: 0363-6399 * page 120, left-hand column, paragraph 3 - middle column, paragraph 4 * * page 124, left-hand column, paragraph 2 - right-hand column, paragraph 3 * * figure 2 *	23-41	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	30 January 2004	Kopp, K

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 98 11 8486

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1-22

Claims 1-22 relate to an apparatus and a method for managing and delivering at laest one document over an electronic network to a recipient.

---

2. claims: 23-41

Claims 23-41 relate to an apparatus and a method for generating a digital certificate

---

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 11 8486

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

30-01-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5390247 A		CA 2093094 A1	07-10-1993
		DE 69329869 D1	22-02-2001
		DE 69329869 T2	16-08-2001
		DK 565314 T3	19-03-2001
		EP 1031908 A2	30-08-2000
		EP 0565314 A2	13-10-1993
		ES 2153371 T3	01-03-2001
		GR 3035527 T3	29-06-2001
		JP 6295286 A	21-10-1994
		PT 565314 T	31-05-2001
		US 5337360 A	09-08-1994
EP 0328232 A	16-08-1989	US 4868877 A	19-09-1989
		AT 122190 T	15-05-1995
		AU 2512488 A	07-09-1989
		CA 1331213 C	02-08-1994
		DE 68922422 D1	08-06-1995
		DE 68922422 T2	07-09-1995
		EP 0328232 A2	16-08-1989
		ES 2071651 T3	01-07-1995
		US 5005200 A	02-04-1991
		US 5214702 A	25-05-1993

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82